Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di giustizia UFG
Ambito direzionale Diritto pubblico

31/08/2022

Revisione totale dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD)

Rapporto sui risultati della procedura di consultazione

BJ-D-BF633401/237

Rapporto sui risultati della procedura di consultazione: revisione totale dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD)

Indice

Rapporto sui risultati della procedura di consultazione: revisione totale dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD)

1 Situazione iniziale

Il 25 settembre 2020 il Parlamento ha adottato la revisione totale della legge federale sulla protezione dei dati. Questa revisione intende non solo adattare il diritto svizzero in materia di protezione dei dati all'era digitale, ma anche garantire un livello di protezione riconosciuto su scala internazionale.

La relativa ordinanza (ordinanza relativa alla legge sulla protezione dei dati, OLPD) comprende le disposizioni esecutive generali riguardanti la legge sulla protezione dei dati e alcune disposizioni su delega legislativa. Si propone come fine principale una migliore esecuzione della legge sulla protezione dei dati grazie a disposizioni più dettagliate e mira ad agevolarne l'applicabilità. Essa si applica al trattamento dei dati sia da parte di privati (in particolare aziende) che da parte di organi federali. Al trattamento dei dati da parte di organi cantonali e comunali si applica invece di norma il diritto cantonale in materia di protezione dei dati.

2 Procedura di consultazione

Il 23 giugno 2021 il Consiglio federale ha avviato la procedura di consultazione sul disegno di ordinanza. La consultazione si è conclusa il 14 ottobre 2021. Sono stati invitati a partecipare i Cantoni, i partiti rappresentati in Parlamento, le associazioni mantello nazionali dei Comuni, delle città e delle regioni di montagna e quelle dell'economia nonché altre cerchie interessate. Nel complesso sono giunti 123 pareri. Tra gli altri, hanno espresso il proprio parere 24 Cantoni[1], la Conferenza degli incaricati della protezione dei dati «privatim», sei partiti[2] e numerose associazioni del mondo economico, della protezione dei consumatori e della protezione dei dati.[3]

Due Cantoni (NE, TI), il Tribunale federale e il Tribunale penale federale hanno espressamente rinunciato ad esprimere un parere. Anche il Cantone di Obvaldo non ha preso posizione, allega tuttavia il parere della sua autorità incaricata della protezione dei dati. Anche l'Unione svizzera degli imprenditori non ha presentato alcun parere, poiché come da ripartizione del dossier il progetto è stato trattato da economiesuisse.

[1] Cantoni: AG, AI, AR, BE, BL, BS, FR, GE, GL, GR, LU, NE, NW, OW, SG, SH, SO, SZ, TG, TI, UR, VD, VS, ZH. Assenti: JU, ZG.

[2] Partiti: Alleanza del centro, PLR, I VERDI, PPS, PS, UDC.

[3] come ad esempio organizzazioni: DigiGes, economiesuisse, sgv, SwissHoldings, Fondazione per la protezione dei consumatori.

3 Risultati della procedura di consultazione

3.1 Osservazioni generali

10 Cantoni,[4] 2 partiti[5] e 6 organizzazioni[6] accolgono in linea di massima il progetto, anche se la maggioranza di essi vede ancora margine di miglioramento. Molti Cantoni si fondano sul parere di privatim.

2 Cantoni,[7] 2 partiti[8] e 29 organizzazioni[9] rifiutano in modo netto il disegno o lo vedono in modo molto critico.

Anche altri partecipanti alla consultazione (5 Cantoni,[10] un partito[11] e 44 organizzazioni[12]) si mostrano scettici o critici.

4 Cantoni,[13] il Tribunale amministrativo federale e 11 organizzazioni o persone[14] commentano il progetto e fanno proposte di miglioramento senza schierarsi a favore o contro.

3.1.1 Punti essenziali

Molti partecipanti alla procedura di consultazione sono del parere che per diverse norme[15] manchi la base giuridica[16] e che la volontà legislativa sia stata disattesa, in quanto sono state adottate regolamentazioni contrarie alle delibere parlamentari.[17] Inoltre, il disegno di ordinanza contraddice in parte la nLPD.[18] In questo senso, si desidera che le disposizioni dell'ordinanza facciano chiaro riferimento alle rispettive norme della legge.[19] Inoltre, l'ordinanza non riflette abbastanza chiaramente la linea generale di un approccio basato sui rischi[20] perseguita nella

4 Cantoni: AI, BE, BS, GL, LU, NW, SG, TG, VS, ZH.

5 Partiti: Alleanza del centro, PS.

6 Organizzazioni: DFS, FER, FMH, UPSC, USS, UCS.

7 Cantoni: UR, VD.

8 Partiti: PLR, UDC.

9 Organizzazioni: ABES, Coop, digialswitzerland, economiesuisse, GastroSuisse, HKBB, ASSOCIAZIONE DI COMMERCIO.swiss, HotellerieSuisse, H+, le banche domestiche, Migros, pharmaSuisse, la Posta, Raiffeisen, Rega, Ringier, FFS, Scienceindustries suisse, ASB, SDV, usam, ASA, suva, thurbo, veb.ch, UTP, UBCS, VUD, Walderwyss.

10 Cantoni: AG, AR, GR, SH, SZ.

11 Partito: I VERDI

12 Organizzazioni: UPSA, ADIDE, IS, ASIP, ASPS, asut, auto schweiz, Bär & Karrer, CP, Creditreform, curafutura, CURAVIVA, datenschutzguide.ch, CFC, EXPERTsuisse, ASSOCIAZIONE DI COMMERCIO.swiss IGEM, INSOS, forum PMI, FRC, ATPrD, EPS, Privacy Icons, privatim, proFonds, ASP, santésuisse, FSA, senesuisse, ASSL, BNS, SPA, Spitex Svizzera, SSO, Fondazione per la protezione dei consumatori, SUISA, SWICO, SwissHoldings, swissICT, Swiss Insights, SwissFoundations, swissstaffing, Sunrise UPC, vsi, VSP.

13 Cantoni: BL, FR, GE, SO.

14 Organizzazioni: ASDPO, Bibliosuisse, Classtime, CYBER SAFE, DigiGes, biblioteca dell'ETH, HÄRTING Rechtsanwälte, HDC, Swimag, swissprivacy.law, privato: Beat Lehmann.

15 Art. 1 cpv. 2, art. 3, art. 4, art. 5, art. 6 cpv. 2, art. 9 cpv. 1 lett. j e k, art. 15, art. 16, art. 17, art. 18, art. 19 cpv. 1 lett. b-d, cpv. 2, cpv. 3 e cpv. 5, art. 20 cpv. 5, art. 31 e art. 32 AP-OLPD.

16 Cantoni: BE, SZ, UR, VD (per quanto riguarda il trattamento di dati personali degni di particolare protezione); partiti: UDC; organizzazioni: UPSA, asut, Bär & Karrer, Coop, Creditreform, Datenschutzguide.ch, le banche domestiche, la Posta, economiesuisse, EXPERTsuisse, GastroSuisse, H+, HKBB, HotellerieSuisse, IGEM, forum PMI, Migros, pharmaSuisse, Raiffeisen, rega, Ringier, FSA, ASB, usam, ASSL, BNS, SSO, suisa, Sunrise UPC, suva, SWICO, SwissFoundations, SwissHoldings, swissICT, Swiss Insights, swissstaffing, veb.ch, UTP, vsi, UBCS, VUD, Walderwyss.

17 Partiti: UDC; organizzazioni: UPSA, auto schweiz, Coop, Creditreform, le banche domestiche, digitalswitzerland, economiesuisse, EXPERTsuisse, ASSOCIAZIONE DI COMMERCIO.swiss, H+, HKBB, HotellerieSuisse, IGEM, forum PMI, Raiffeisen, rega, Ringier, FSA, Scienceindustries Switzerland, suisa, suva, SWICO, Swiss Insights, SwissHoldings, veb.ch, vsi, VUD.

18 Organizzazioni: Auto schweiz, digitalswitzerland, EXPERTsuisse, Raiffeisen, ASSL, Swiss Insights.

19 Organizzazioni: Creditreform, DFS, IGEM, EPS, ASP, FSA, swissstaffing, vsi, VSP.

20 Per approccio basato sui rischi si intende che gli obblighi del responsabile sono sempre da valutare tenendo conto della natura, della portata, delle circostanze e delle finalità del trattamento nonché delle diverse probabilità di realizzazione e gravità dei rischi per i diritti e le libertà delle persone fisiche.

nLPD.[21] Alcuni partecipanti alla consultazione sono del parere opposto e ritengono che l'AP-OLPD aderisca al quadro della nuova legge federale sulla protezione dei dati (nLPD) e che addirittura lo limitino in riferimento a determinati aspetti.[22] In questo senso, è cruciale che il Consiglio federale continui a usare coerentemente il proprio margine di manovra per una maggiore protezione dei dati e non mini l'articolo 61 lettera c nLPD con misure poco esaustive o troppo vaghe.[23] Pertanto, si auspica che vengano regolamentati ulteriori punti quali ad esempio la valutazione d'impatto sulla protezione, la trasmissione e la portabilità dei dati.[24]

Una critica frequente all'intero avamprogetto è che le disposizioni non sono elaborate con sufficiente precisione, lasciando quindi troppo spazio all'interpretazione e alle ambiguità.[25] Inoltre, si critica l'uso di termini obsoleti e la reintroduzione di disposizioni superate dell'attuale OLPD.[26] Numerose disposizioni della nuova ordinanza non sono quindi in linea con le basi legali della nLPD.[27] Inoltre, alcuni termini imprecisi o vaghi sono stati ripresi ciecamente da varie fonti.[28] Questo porta ad un progetto complessivo confuso e terminologicamente incoerente.[29] Molti partecipanti auspicano che alcune spiegazioni del rapporto esplicativo siano inserite nell'ordinanza stessa.[30]

D'altra parte, si critica il fatto che le disposizioni troppo dettagliate o troppo ampie causerebbero un lavoro eccessivo e porterebbero a conseguenze negative involontarie.[31] In particolare, si osserva che l'obiettivo e il contenuto della valutazione d'impatto sulla protezione dei dati, dei regolamenti di trattamento, dell'elenco delle attività di trattamento e dell'obbligo di registrazione si sovrappongono.[32] In generale, si critica la presenza di sovrapposizioni.[33] I requisiti in parte molto restrittivi non sono realizzabili nella pratica (in particolare per le PMI).[34] Il Cantone di Friburgo considera lodevoli le disposizioni parzialmente flessibili.[35]

---

21 Cantoni: BL; organizzazioni: la Posta, privatim, ASB, UBCS. Il Cantone di VD, invece, riconosce un'attuazione coerente di questo approccio, in particolare nelle disposizioni sulla sicurezza dei dati.

22 Organizzazioni: DigiGes

23 Partito: UDC; organizzazioni: FRC, USS.

24 p. es. partiti: I VERDI, PS; organizzazioni: DigiGes, FRC, USS, Fondazione per la protezione dei consumatori.

25 Cantoni: AG, AR, GL GR, NW SH, VD; organizzazioni: CYBER SAFE, responsabile della protezione dei dati SZ/OW/NW, digitalswitzerland, economiesuisse, FRC (relativo al profiling ad alto rischio e alla protezione dei dati attraverso la tecnologia e le impostazioni predefinite favorevoli alla protezione dei dati), ASSOCIAZIONE DI COMMERCIO.swiss, HKBB, ATPrD, pharmaSuisse, privatim, Raiffeisen, Scienceindustries Switzerland, Fondazione per la protezione dei consumatori, veb.ch.

26 Cantoni: GR, SH, VD; organizzazioni: privatim, Ringier.

27 Organizzazioni: DFS, FMH, H+, HKBB, Migros, FSA.

28 Organizzazioni: CP, CURAVIVA, la Posta, DFS, CFC, FMH, H+, ASSOCIAZIONE DI COMMERCIO.swiss, INSOS, santésuisse, senesuisse, BNS, Fondazione per la protezione dei consumatori.

29 Organizzazioni: DFS, FMH, H+, HKBB, Migros, FSA.

30 Organizzazioni: DFS, ATPrD.

31 Cantoni: SZ, ZH; imprese: Coop, la Posta, digitalswitzerland, economiesuisse, FMH, H+, IGEM, proFonds, SWICO, UBCS, VUD, Walderwyss.

32 p. es. organizzazioni: SWICO.

33 Organizzazioni: Auto schweiz, santésuisse, BNS.

34 Partiti: UDC; organizzazioni: Bär & Karrer, digitalswitzerland, H+, ASSOCIAZIONE DI COMMERCIO.swiss, HKBB, FSA, Scienceindustries Switzerland, SwissFoundations, thurbo, Walderwyss.

35 Anche l'organizzazione: CP.

Si critica inoltre che l'ordinanza presenta molte peculiarità svizzere non previste dalla legge e che vanno anche oltre il Regolamento europeo sulla protezione dei dati RGPD (swiss finish[36]).[37] Soprattutto in relazione ai cosiddetti swiss finish, il tenore è che questi porterebbero spesso a spese eccessive per il settore privato e quindi a uno svantaggio competitivo per le imprese svizzere.[38]

Indipendentemente da questo, si criticano anche le lacune del regime transitorio della nLPD. In particolare, ci dovrebbero essere adeguati periodi di transizione per ogni nuovo obbligo introdotto nell'ordinanza.[39] Tuttavia, bisogna fare attenzione a garantire una valutazione dell'adeguatezza della Commissione europea.[40] Tra i commenti positivi, viene accolta con favore l'armonizzazione con il diritto europeo.[41]

Si elogia anche la migliore strutturazione e sistematicità, così come il linguaggio più chiaro.[42] Un altro punto accolto con favore è la concretizzazione del diritto d'informazione.[43] CP osserva che le nuove regole sono un prerequisito per l'accettazione sociale della digitalizzazione e dell'innovazione, che diventeranno sempre più importanti nei prossimi anni e rappresentano un elemento cruciale del progresso economico della Svizzera.[44] Costituiscono inoltre anche un'occasione per le imprese di ottimizzare i loro processi.[45]

3.1.2 Osservazioni generali

3.1.2.1 Sulla sicurezza dei dati

L'intera sezione (art. 1-5) è oggetto di molte critiche. È considerata imprecisa e poco dettagliata. Si manifesta anche la preoccupazione che l'uso di concetti giuridici indeterminati possa indebolire la portata della protezione nonché la possibilità di ricorrere a disposizioni penali. Le disposizioni sono inoltre criticate in quanto troppo dettagliate. In alcuni casi sono messe in discussione la struttura e le scelte terminologiche. Si sottolinea spesso anche la mancanza di una base legale.

La sezione incontra anche giudizi positivi. L'approccio basato sui rischi è sostenuto da un gran numero di partecipanti[46]. La struttura scelta è accolta con favore da alcuni partecipanti[47], in particolare la differenza a seconda del tipo e delle attività dell'impresa. Bär & Karrer comprende anche la riluttanza del Consiglio federale a introdurre requisiti minimi specifici nell'ordinanza e

[36] Uno swiss finish è una regolamentazione svizzera che va oltre i requisiti della legislazione UE, in questo contesto il GDPR, senza creare per i partecipanti svizzeri un vantaggio nel mercato UE. Al contrario, gli swiss finish sono solitamente considerati uno svantaggio competitivo per le aziende svizzere.

[37] Organizzazioni: UPSA, asut, auto schweiz, Creditreform, la Posta, economiesuisse, EXPERTsuisse, ASSOCIAZIONE DI COMMERCIO.swiss, HKBB, forum PMI, Migros, EPS, Raiffeisen, Ringier, ASP, FSA, ASB, Scienceindustries Switzerland, usam, ASSL, Sunrise UPC, SwissHoldings, Swiss Insights, swissstaffing, vsi, UBCS, VSP.

[38] Organizzazioni: asut, la Posta, digitalswitzerland, EXPERTsuisse, FER, HKBB, forum PMI, Migros, Ringier, FSA, Scienceindustries Switzerland, Sunrise UPC, SWICO, SwissHoldings, UBCS.

[39] Organizzazioni: ASIP, Coop, curafutura, la Posta, IGEM, pharmaSuisse, Raiffeisen, rega, FSA, usam, ASA, swissstaffing, VUD, Walderwyss.

[40] Organizzazioni: asut, digitalswitzerland, FER, HotellerieSuisse, forum PMI, Ringier, UPSC, ASSL, SwissHoldings.

[41] Organizzazioni: Digitalswitzerland, H+, ASSL, BNS, UCS.

[42] Cantoni: VS; organizzazioni: VIPD.

[43] Partiti: Alleanza del centro, organizzazioni: Fondazione per la protezione dei consumatori.

[44] Anche le organizzazioni: UPSC, GastroSuisse.

[45] Organizzazioni: CP, UPSC.

[46] Cantoni: AG, BE, BL, GL, LU, NW, OW, SO, SZ, ZH; organizzazioni: ASA, ASP, ASSL, ATPrD, FFS, Creditreform, curafutura, Datenschutzguide.ch, digitalswitzerland, economiesuisse, H+, HKBB, la Posta, le banche domestiche, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, Raiffeisen, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, vsi. L'approccio basato sui rischi richiede tuttavia alcuni adeguamenti.

[47] Organizzazioni: ATPrD, Bär & Karrer.

accoglie con favore il rafforzamento della sicurezza dei dati. Alcuni Cantoni[48] accolgono la formulazione aperta delle disposizioni, che ne permette un'ampia attuazione. Tuttavia, LU è del parere che la pronuncia di una multa sulla base della violazione di queste disposizioni sia inappropriata. Alla luce del principio della certezza del diritto, si chiede un chiarimento della relazione tra le disposizioni di questa prima sezione e l'articolo 61 nLPD. Secondo l'UPSC, una formulazione generale apporta dei vantaggi. Tuttavia, mette in discussione la libertà di interpretazione lasciata alla giurisprudenza. Tale delega al potere giudiziario rappresenta una possibile violazione del principio della separazione dei poteri. Propone una terminologia più distintiva. H+ accoglie con favore lo sviluppo di requisiti minimi poco rigidi, ricordando che sarebbe difficile fissare dei requisiti generali applicabili a tutti i settori. VS è favorevole ai requisiti minimi da rispettare per la sicurezza dei dati. Comprende che queste «linee guida» siano da intendersi in maniera flessibile.

Nelle loro considerazioni generali, molti partecipanti[49] sono del parere che il progetto non soddisfa i requisiti minimi (art. 8 nLPD). Il principio di legalità nel diritto penale richiede che un atto sia espressamente menzionato dalla legge per poter essere punibile (art. 8 cpv. 3 e 61 cpv. 1, lett. c nLPD). Il progetto non definisce con sufficiente precisione l'assenza di quale misura costituirebbe un reato. Le misure minime devono essere dettagliate. H+ rifiuta le disposizioni di questa sezione, ritenendole prive di base legale. Essendo troppo dettagliate e non tenendo conto delle diverse attività di trattamento e situazioni, con il rischio di creare un sovraccarico amministrativo, sono in contraddizione con la volontà del legislatore. Altri partecipanti[50] sono della stessa opinione. Inoltre, deplorano il fatto che i concetti dell'attuale OLP siano stati ripresi e semplicemente completati con principi del diritto europeo[51]. Chiedono al Consiglio federale di rivedere l'intera sezione, citando come esempio la legge del 18 dicembre 2020[52] sulla sicurezza delle informazioni. Alcuni partecipanti[53] propongono di rifarsi all'articolo 32 paragrafo 1 RGPD o di specificare le misure.

VD propone di includere in questa prima sezione dei criteri che indichino la pertinenza, o addirittura l'obbligo, di condurre delle valutazioni d'impatto relativa alla protezione dei dati (VIPD), al fine di concretizzare e sviluppare la nozione di rischio elevato per la personalità o i diritti fondamentali della persona interessata dell'articolo 16 capoverso 1 nLPD.

Alcuni partecipanti[54] chiedono di non svuotare queste disposizioni del loro senso mediante misure troppo modeste o poco esplicite. Lamentano anche l'uso di concetti giuridici imprecisi[55].

---

48 Cantoni: FR, LU.

49 Cantoni: AI ; partito: PVS; organizzazioni: ASDPO, FRC, HDC, Swissprivacy, UBCS, veb.ch. Altri partecipanti condividono questo punto di vista soprattutto per quanto riguarda l'art. 2. Su questo argomento, cfr. nbp n. 98.

50 Cantoni: AG, AR, BE, GL, GR, NW, SH, SZ, VD, ZU, PVS. VD sostiene la richiesta di revisione e insiste in particolare sull'articolo 1, capovero 1; partito: PVS; organizzazioni e privati: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, Ringier; privato: Beat Lehmann.

51 Su questo argomento, cfr. nbp n. 97.

52 LSIn, RU **2020** 232.

53 Cantoni: AG, AR, BE, GL, NW, SH, SZ, VD, ZH; organizzazioni: ATPrD, Bär & Karrer, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim. Su questo argomento, cfr. nbp n. 60.

54 Organizzazioni: DigiGes, FRC, Fondazione per la protezione dei consumatori.

55 A questo proposito, si vedano i commenti all'art. 1, cpv. 2, e all'art. 2, frase introduttiva.

3.1.2.2 Sulla comunicazione di dati personali all'estero

GL accoglie con favore l'insieme delle disposizioni della sezione (art. 8-12), che possono servire da ispirazione per il diritto cantonale. Alcuni partecipanti[56] ricordano l'importanza di queste disposizioni e giudicano i requisiti pertinenti.

3.2 Pareri sulle singole disposizioni

3.2.1 Art. 1 AP-OLPD: principi

Due partecipanti accolgono con favore i principi introdotti in questo primo articolo[57].

Cpv. 1

Diversi partecipanti[58] accolgono con favore la formulazione di questa disposizione, che secondo loro attua in modo ottimale l'articolo 8 capoverso 1 nLPD. Tuttavia, la libertà di interpretazione richiede un sostegno specifico nella pratica. Si suggerisce di aggiungere, in un nuovo capoverso, che «l'IFPDT deve creare quanto prima dei documenti che semplificano l'attuazione pratica». Al contrario, il DFS ritiene che la formulazione non rispetti l'articolo 8 capoverso 1 nLPD. Propone di aggiungere l'articolo 8 capoverso 1 nLPD come frase introduttiva all'articolo 1. Per quanto riguarda i criteri, sarebbe giustificato menzionare «in particolare». La FMH propone di aggiungere nell'introduzione «vanno adottate misure tecniche e organizzative appropriate per garantire un livello di sicurezza adeguato al rischio». L'ASDPO chiede di specificare che le misure minime possono essere selezionate dalla lista dell'articolo 2. Classtime vorrebbe aggiungere «l'utilità del trattamento» all'articolo 1.

Alcuni partecipanti ritengono che[59] vada garantita l'uniformità terminologica: i provvedimenti non sono «adeguati», bensì «appropriati» secondo l'articolo 8 capoverso 1 nLPD. Inoltre, sono del parere che l'attuazione dell'articolo 8 nLPD vada oltre la sicurezza dei dati in senso stretto (CAID: confidenzialità, autenticità, integrità, disponibilità). In questo senso, considerano sbagliati gli esempi citati e la portata del termine «rischio». Si tratta di un rischio netto e non di un rischio lordo. Quindi il trattamento da parte dell'intelligenza artificiale (IA) o degli esseri umani non è rilevante per la questione della sicurezza dei dati.

In linea generale, molti partecipanti[60] notano l'influenza del diritto europeo, in particolare dell'articolo 32 RGPD. Propongono di ispirarsi ad esso e alla LSIn. Ritengono che l'approccio dovrebbe essere duplice: in primo luogo, valutare gli obiettivi e le necessità di protezione nonché i rischi. Anche se gli obiettivi di protezione sono stabiliti nell'articolo 5 capoverso 1 lettera h nLPD e elencati in modo dettagliato nell'articolo 2, si apprezza la distinzione operata in questo capoverso tra i criteri di valutazione del bisogno di protezione (lett. a), di valutazione del rischio (lett. b) e l'adeguatezza delle misure. Tuttavia, come per la valutazione dell'impatto relativa alla protezione dei dati, la valutazione dei rischi avviene in una fase successiva (art. 22 nLPD). In merito ai criteri di adeguatezza delle misure, i partecipanti lamentano il loro carattere indiretto. L'opportunità di una misura dovrebbe permettere di valutare se una misura vada adottata e, in

[56] Partito: PS; organizzazioni: USS.

[57] Organizzazioni: ASDPO, FER.

[58] Cantoni: VD; organizzazioni: Assistenza e cura a domicilio ASPS, CURAVIVA.CH, INSOS, IS, senesuisse. Il forum PMI sostiene la necessità di sostegno da parte dell'IFPDT, ma con una visione più critica del progetto. Il CP propone lo stesso approccio, in particolare per le nuove definizioni aggiunte nella nLPD, inclusa la «profilazione a rischio elevato».

[59] Organizzazioni: FFS, FSA, H+, IGEM, la Posta, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[60] Cantoni: AG, AR, BE, GL, NW, SH, SZ, VD, ZH; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

concreto, quale misura contrasterà il rischio con l'efficacia necessaria. Due Cantoni[61] considerano anche lo «stato della tecnica» come un criterio indiretto. SZ si chiede se i criteri di adeguatezza siano cumulativi; caratteristica che considererebbe negativa. Anche ZH si oppone a questo carattere cumulativo. Sottolinea che la definizione degli obiettivi di protezione (art. 5 lett. h nLPD), la necessità di protezione (art. 1 cpv. 1 lett. a) e i rischi (art. 22 nLPD) andrebbero resi più chiari.

BL propone di armonizzare la metodologia analogamente alla Confederazione mediante HERMES. L'articolo 1 dovrebbe quindi riflettere la valutazione dei rischi e le misure da adottare secondo lo stato attuale delle conoscenze tecniche.

Il PS ritiene che il rischio di una violazione della sicurezza dei dati sia un criterio di valutazione molto più rilevante per le misure da adottare.

Cpv. 1 lett. a

VD propone di inserire alla lettera a «criteri relativi alla profilazione, ai trasferimenti internazionali e all'outsourcing (cloud)».

Per quanto riguarda il contenuto, SPA contesta il legame tra i criteri menzionati e il rischio posto dal trattamento dei dati. Propone di menzionare espressamente i criteri in base ai quali si può stabilire un rischio ai sensi dell'articolo 8 capoverso 1 nLPD. Un altro partecipante[62] chiede la cancellazione del termine «circostanze», considerandolo incluso nel termine «tipo» del trattamento dei dati. Inoltre, propone di prendere in considerazione il progetto della Commissione europea relativo al Regolamento sull'intelligenza artificiale.

Cpv. 1 lett. b

Diversi partecipanti[63] sono del parere che i costi di attuazione andrebbero presi in considerazione in conformità con l'articolo 1, capoverso 1, lettera b; vale a dire quando si valuta l'adeguatezza di una misura e non solo quando si decide quale misura è appropriata. Alcuni partecipanti[64] suggeriscono di aggiungere che la probabilità ha senso solo in presenza di un rischio. Quest'ultimo deriva da una potenziale violazione della sicurezza dei dati, e non viceversa. In questo senso, il testo dovrebbe essere il seguente: «potenziali effetti successivi di una violazione della sicurezza dei dati sulle persone interessate e la loro probabilità».

Si sottolinea che la probabilità è un calcolo matematico[65]. Così la classificazione proposta non può essere seguita (bassa, media o elevata). Bisognerebbe sostituire il termine «probabilità» con «conseguenze», se non addirittura introdurre criteri matematici.

Alcuni partecipanti[66] chiedono di tenere conto del rischio residuo.

[61] Cantoni: NW, SZ.

[62] Organizzazione: DFS.

[63] Organizzazioni: ASSL, auto suisse, SwissInsights, UPSA.

[64] Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, swissICT.

[65] Organizzazione: Associazione di commercio.

[66] Organizzazioni: HÄRTING, suva, swissICT.

Cpv. 1 lett. c

Lo stato della tecnica deve essere verificato. In tal senso andrebbe aggiunto come criterio lo «stato della scienza», poiché da anni esso è universalmente riconosciuto[67]. HÄRTING chiede alcuni chiarimenti sul termine «stato della tecnica», in particolare in relazione alle sanzioni penali dell'articolo 61 lettera c nLPD e propone di sostituirlo con «le regole generali della tecnica».

Cpv. 1 lett. d

Diversi partecipanti[68] criticano l'inclusione delle spese e suggeriscono di cancellare la lettera d o di riformulare questa disposizione. La necessità di precisione è ripetutamente espressa, per esempio, in relazione alle «spese di implementazione» per PMI, fondazioni, piccole e medie associazioni o start-up (in relazione al tetto dei costi tra la cifra d'affari (prevista) e le spese di implementazione). Pur affermando che questo criterio riguarda solo la scelta della variante più conveniente - tra quelle ritenute efficaci -, si sottolinea che non è né un lasciapassare né una deroga all'obbligo di garantire la sicurezza dei dati. Al contrario, questo criterio deve permettere di soddisfare questi requisiti, soprattutto per le piccole e medie imprese[69]. Alcuni partecipanti[70] considerano inoltre che le «spese di implementazione» implicano erroneamente che le altre spese non siano rilevanti. Il rapporto esplicativo non dovrebbe affermare che spese eccessive non siano utili.

Molti partecipanti[71] suggeriscono di sostituire «spese di implementazione» con «sforzo di implementazione», poiché ritengono che il primo termine sia troppo limitato. BE afferma, inoltre, che altri criteri di attuazione possono essere rilevanti (oneri elevati in termine di personale o in termine di tempo e organizzazione). Così facendo, il rapporto esplicativo guadagnerebbe una maggiore precisione. Altri partecipanti[72] condividono questo punto di vista e si rammaricano dell'imprecisione delle spiegazioni relative all'inclusione delle spese di implementazione come criterio nella valutazione dell'adeguatezza. A questo proposito, ProFonds sottolinea che l'adeguatezza della misura deve essere valutata non solo sulla base delle spese di implementazione, ma anche alla luce di tutti gli altri costi. Alcuni partecipanti[73] aggiungono lo sforzo generale di implementazione. Per alcuni partecipanti[74], in virtù del principio di proporzionalità, bisognerebbe tenere conto anche delle altre spese. Non è quindi necessario menzionarle esplicitamente.

Diversi partecipanti[75] accolgono con favore le spese di implementazione come criterio di adeguatezza, ritenendo positivo che lo sforzo per i responsabili sia chiaramente incluso. Propongono, tuttavia, di sostituirlo con «spese per i responsabili».

---

67 Organizzazione: Swimag.

68 Partiti: PVS, PS; organizzazione: USS.

69 Organizzazioni: Associazione di commercio, HotellerieSuisse, PES, proFonds, UPSC.

70 Organizzazioni: Associazione di commercio, FFS, CSPreditreform, H+, la Posta, Migros, proFonds, Ringier, SPA, suva, thurbo, UTP, VUD, Walderwyss.

71 Cantoni: BE; organizzazioni: ASB, ASSL, Bär & Karrer, FMH, la Posta, Raiffeisen, Ringier, santésuisse, suva, swissICT, swissstaffing, UPSA, usam, vsi, VUD.

72 Organizzazioni: ASSL, PES, SPA, UPSA.

73 Organizzazioni: ASSL, auto suisse, FSA, SwissInsights, UPSA.

74 Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, SDV, Scienceindustries suisse, swissICT.

75 Organizzazioni: ASP, Creditreform, EPS, VSP, vsi.

Due partecipanti[76] fanno notare che non è saggio menzionare esplicitamente le spese di implementazione come criterio di valutazione dell'adeguatezza dei provvedimenti nell'ordinanza. Il rischio di una violazione della sicurezza dei dati è il criterio di valutazione pertinente per le misure da adottare. Swimag, al contrario, vorrebbe una formulazione precisa che includa l'aggiunta dei mezzi minimi da implementare, lo sforzo e le spese.

Cpv. 2

Si chiede la cancellazione di questo capoverso[77]. Molti partecipanti[78] chiedono almeno di sostituire «a intervalli adeguati» con «in modo adeguato». Secondo SZ, questi «intervalli adeguati» non sono molto efficaci; sarebbe più appropriato optare per «i provvedimenti devono essere verificati in modo globale». Altri partecipanti[79] ritengono inoltre il termine «intervallo adeguato» aperto all'interpretazione e suggeriscono di sostituirlo con «intervallo periodico». Alcuni partecipanti[80] chiedono più chiarezza e insistono per una verifica almeno una volta all'anno. La Fondazione per la protezione dei consumatori propone un «intervallo periodico e adeguato». Alcuni[81] chiedono che i provvedimenti siano verificati «in caso di cambiamenti tangibili dei rischi». L'Associazione di commercio specifica che i provvedimenti andrebbero verificati solo se cambiassero le condizioni dell'articolo 1 capoverso 1 lettere a-c. Altri partecipanti[82] ritengono che il responsabile sia il solo in grado di valutare l'adeguatezza della verifica nell'arco di tutto il trattamento. Alcuni partecipanti[83] mettono in dubbio il legame tra l'articolo 8 capoverso 3 nLPD e questo requisito aggiuntivo di «verifica a intervalli adeguati». Secondo alcuni partecipanti[84], la verifica dovrebbe avere luogo di continuo. La FRC afferma che la frequenza non deve essere soggetta a interpretazioni.

Per quanto riguarda la terminologia, si preferisce «valutazione dei rischi» rispetto a «provvedimenti»[85]. Alcuni partecipanti[86] fanno notare che la revisione si concentra sui fattori di rischio. BE propone di precisare che «i rischi e i provvedimenti sono verificati».

EXPERTsuisse raccomanda di rendere obbligatoria la norma ISO 27001 per standardizzare il controllo.

Infine, è necessario allinearsi al diritto europeo e internazionale e fare una distinzione per i dati archiviati[87].

---

[76] Partito: PS; organizzazione: USS.

[77] Organizzazione: SPA

[78] Organizzazioni: ASSL, ASB, auto suisse, FFS, digitalswitzerland, economiesuisse, FSA, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, SPA, SSO, suva, SwissInsights, swissstaffing, thurbo, UPSA, UTP, VUD, Walderwyss.

[79] Organizzazioni: santésuisse, UPSC.

[80] Organizzazioni: Assistenza e cura a domicilio, ASPS, CURAVIVA.CH, INSOS, IS, senesuisse.

[81] Organizzazioni: ASP, Creditreform, EPS, VSP, usam, vsi.

[82] Organizzazioni: SwissICT, Walderwyss.

[83] Organizzazioni: ASP, Creditreform, EPS, VSP, vsi.

[84] Cantoni: AG, BE, GL, NW, VD; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[85] Cantoni: BE, GL; organizzazioni: ATPrD, FMH, privatim.

[86] Cantoni: BE; organizzazione: DigiGes.

[87] Privato: Beat Lehmann.

3.2.2 Art. 2 AP-OLPD: Obiettivi di protezione

La disposizione ha riscosso qualche parere positivo. Alcuni partecipanti[88] accolgono con favore l'elenco degli obiettivi, che funge da promemoria. Tuttavia, sottolineano la necessità di un sostegno ad hoc da parte delle autorità competenti, in particolare l'IFPDT. Propongono di introdurre nel testo di legge che alle imprese svizzere è offerto l'accesso, a costi ragionevoli, all'IFPDT; come minimo, questo catalogo (promemoria) andrebbe inserito in un allegato[89].

Alcuni partecipanti[90] ritengono che i requisiti elencati all'articolo 2 siano quelli volti a garantire gli obiettivi di protezione. È pertanto giustificato ispirarsi all'articolo 6 capoverso 2 LSIn e modificare la frase introduttiva. Poiché gli obiettivi di protezione sono delle finalità, le misure devono essere adeguate ai rischi identificati nella relativa valutazione dei rischi. Alcuni partecipanti[91] suggeriscono, ad esempio, di ispirarsi alla legge sull'informazione e la protezione dei dati dei Cantoni BS e ZH.

La disposizione è, tuttavia, ampiamente criticata. Molti partecipanti[92] ritengono indispensabile operare una revisione. Sebbene si apprezzi l'influenza esercitata dall'articolo 5 capoverso 1 lettera h nLPD o dall'articolo 32 paragrafo 1 RGPD, gli obiettivi menzionati devono essere limitati alla confidenzialità, integrità, disponibilità e tracciabilità. L'intento è quello di fissare dei requisiti minimi. Inoltre, l'allineamento con il diritto dell'UE faciliterà l'attuazione della nLPD e del RGPD[93]. In quest'ottica, alcuni partecipanti[94] chiedono l'abolizione di tutti gli swiss finish. Dalla disposizione deriva un obbligo di documentazione contrario all'intenzione del legislatore[95]. Per SPA, tale documentazione non è legittima e si giustifica solo in parte per il processo e il suo risultato. Si critica la ripresa degli obiettivi dell'OLPD vigente[96], che alcuni partecipanti ritengono superati[97]. Inoltre, il DFS ritiene indispensabile il contributo pratico di esperti del campo dell'informazione e della protezione dei dati nel processo di revisione di questa disposizione.

Secondo alcuni partecipanti[98], l'articolo 2 non adempie pienamente il mandato stabilito dall'articolo 8 capoverso 3 nLPD. Diversi partecipanti[99] sottolineano che la disposizione dovrebbe menzionare solo gli obiettivi di protezione che il responsabile può influenzare. Fanno notare che l'introduzione della «privacy by design» costringe il responsabile ad occuparsi della sicurezza dei dati. Alla luce dei progressi tecnologici e in assenza di qualsiasi intervento statale, l'elenco va rivisto, in quanto scarica la responsabilità della sicurezza dei dati sull'operatore e

---

88 Organizzazioni: Assistenza e cura a domicilio, ASPS, CURAVIVA.CH, INSOS, IS, senesuisse.

89 Privato: Beat Lehmann.

90 Cantoni: AG, BE, GL, SH, VD, ZH; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

91 Cantoni: AR, NW, SZ; organizzazione: Incaricato cantonale della protezione dei dati SZ, OW e NW.

92 Cantoni: AG, BE, AR, GL, NW, SZ, TG, VD, ZH; partiti: PLR, PS; organizzazioni: ASB, asut, FFS, Coop, DFS, digitalswitzerland, economiesuisse, EXPERTsuisse, FMH, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, SPA, Sunrise, UPC, suva, SWICO, thurbo, UBCS, UTP, veb.ch, VUD, Walderwyss. Secondo swissICT, la confidenzialità, l'integrità, la disponibilità e la tracciabilità dovrebbero almeno essere incluse nei commenti del rapporto esplicativo sull'articolo 2; persona privata: Beat Lehmann propone di creare un capoverso 1 «in generale», che includerebbe confidenzialità, integrità, disponibilità e tracciabilità come obiettivi da raggiungere.

93 Organizzazione: FSA.

94 Organizzazioni: ASB, asut, digitalswitzerland, economiesuisse, forum PMI, HKBB, la Posta, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, Sunrise UPC, SWICO.

95 Organizzazioni: Associazione di commercio, Coop, IGEM, la Posta, suva, Rega, VUD. Alcuni, tra cui SPA, sostengono che non tutti questi obiettivi sono necessariamente pertinenti. Quindi, deve essere possibile determinare, sulla base del trattamento, quale obiettivo è rilevante e quale non lo è.

96 Su questo argomento, cfr. nbp n. 50.

97 Organizzazioni: DFS, IGEM.

98 Partito: PLR; organizzazioni: Datenschutzguide.ch, forum PMI, SPA, suiSA, SwissFoundations.

99 Organizzazioni: ASP, Creditreform, EPS, VSP, usam, vsi.

non sullo sviluppatore delle tecnologie dell'informazione, il tutto a scapito degli utenti di queste tecnologie. Gli attuali attacchi informatici rendono irrealistici obiettivi così ampi e ambiziosi, soprattutto alla luce delle sanzioni penali della nLPD[100].

Alcuni partecipanti[101] si chiedono se vada chiarito il legame con l'articolo 1, o almeno il fatto che vanno implementati solo gli elementi necessari a garantire un'adeguata sicurezza dei dati.

BE ritiene che la frase introduttiva debba specificare «misure tecniche e organizzative». Una vasta maggioranza dei partecipanti[102] suggerisce di sostituire «soddisfare» con «sforzarsi di raggiungere», soprattutto alla luce dell'articolo 61 lettera c nLPD. Il PVS sottolinea che gli obiettivi vanno raggiunti solo «per quanto possibile», lasciando ai responsabili un margine di discrezione che può essere contrario alla sicurezza dei dati. Datenschutzguide.ch considera centrale questa integrazione circostanziale. L'attuazione di molti obiettivi può risultare difficile per le PMI. Bisogna porre l'accento su dei requisiti minimi. Non può trattarsi di un elenco dettagliato passibile di multe. Alcuni partecipanti[103] ritengono che la suddetta locuzione non sia necessaria alla luce dell'articolo 6 capoverso 5 nLPD, soprattutto perché tende a relativizzare gli obiettivi da raggiungere. Diversi partecipanti[104] ne propongono l'eliminazione, poiché soggetta a interpretazione. Due partecipanti[105] chiedono una maggiore spiegazione dell'espressione «per quanto possibile», poiché il rapporto esplicativo non è di grande aiuto.

Swimag ritiene opportuno aggiungere «almeno» prima di «i seguenti obiettivi di protezione». GR propone invece di aggiungere «in particolare» per non comprendere l'elenco in modo esaustivo. DFS ritiene che un elenco esaustivo non abbia senso, poiché si tratta di provvedimenti tecnici e organizzativi e non di obiettivi. Il PPS vorrebbe una distinzione tra le imprese che trattano i dati solo in modo amministrativo e le imprese il cui modello di business è basato sulla raccolta, l'analisi, la fornitura e/o l'utilizzo di dati. Al fine di prevenire gli abusi, a queste ultime imprese andrebbe ulteriormente limitata questo margine di valutazione.

Secondo le banche domestiche, la realtà del mercato economico svizzero richiede più precisione.

Gli obiettivi di protezione vanno interpretati in base al loro contesto e in relazione al livello di sensibilità dei dati[106]. La formulazione deve rendere chiaro che un approccio che tende a questi obiettivi è sufficiente. Si tratta di obiettivi generali, poiché il rischio zero non esiste[107]. In tal senso, il rapporto esplicativo contiene un elenco di obiettivi di protezione sui quali devono concentrarsi i provvedimenti. È possibile che non tutti gli obiettivi di protezione sono rilevanti in ogni caso specifico e vadano quindi adattati[108]. Una nuova struttura potrebbe facilitare questa comprensione. HÄRTING propone di introdurre un capoverso «in generale»[109] e un capoverso

[100] Partito: PLR; organizzazioni: la Posta, rega.

[101] Cantoni: BE; organizzazioni: ASB, ASDPO, Associazione di commercio, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, swissICT.

[102] Cantoni: BE; organizzazioni: ASP, asut, FFS, Coop, Creditreform, DigiGes, EPS, VSP, GastroSuisse, H+, IGEM, la Posta, Migros, Raiffeisen, Ringier, santésuisse, SSO, SPA, Fondazione per la protezione dei consumatori, SUISA, Sunrise UPC, suva, SWICO, swissICT, swissstaffing, thurbo, UTP, VUD, Walderwyss.

[103] Partito: PS; organizzazioni: Fondazione per la protezione dei consumatori, USS.

[104] Partito: PS; organizzazioni: ASDPO, DigiGes, FRC, PES, PPS.

[105] Organizzazioni: CFC, DigiGes.

[106] Organizzazione: Classtime.

[107] Organizzazioni: ASP, BNS, Creditreform, EPS, VSP, usam, vsi; privato: Beat Lehmann.

[108] Organizzazione: HÄRTING.

[109] Su questo argomento, cfr. nbp n. 92.

«mezzi di attuazione degli obiettivi», cioè una clausola generale che indichi le misure organizzative e tecniche a disposizione dei responsabili del trattamento o dell'outsourcing per raggiungere gli obiettivi di protezione, nella quale elencare i mezzi appropriati.

Ringier raccomanda di inserire nell'ordinanza l'elenco degli obiettivi (integrità, confidenzialità e disponibilità), poiché la violazione dei requisiti in materia di protezione dei dati può avere conseguenze rilevanti (sanzioni penali secondo l'art. 61 lett. c nLPD).

HÄRTING suggerisce di aggiungere, in una nuova lettera j, un obbligo di responsabilità all'interno dell'impresa in caso di mancato rispetto degli obiettivi e di prevedere, in una nuova lettera m, un controllo continuo del miglioramento della sicurezza dei dati che tenga conto della costante evoluzione tecnologica.

Titolo

Bär & Karrer propone di modificare il titolo dell'articolo 2 con l'espressione seguente: «requisiti minimi».

Lett. a

Secondo Swimag, l'esperienza dimostra che il numero di persone autorizzate tende ad aumentare senza motivo apparente, soprattutto per i trattamenti che esulano dai loro compiti. È pertanto del parere che la lettera a debba specificare che il numero di persone autorizzate va ridotto al minimo. Va anche aggiunto che l'accesso è limitato ai dati di cui si ha «assolutamente e imperativamente» bisogno.

Lett. b

Secondo la Suva, ad essere interessate sono anche le installazioni «mobili», in particolare gli smartphone e i tablet. Sebbene ASA riconosca che questo risulta anche dal rapporto esplicativo, è del parere che questo tipo di controllo non sia possibile e rientri nel controllo di cui alla lettera a. Si chiede un chiarimento, in particolare nel rapporto esplicativo[110]. La formulazione è troppo ampita e irrealistica (inconciliabile per esempio con il telelavoro durante la pandemia). Risulta giustificato porre l'accento sull'impossibilità di accesso per le persone non autorizzate.

Swimag propone di completare il testo nel seguente modo: «l'accesso ai locali e agli impianti fisici e virtuali [...] è subito rifiutato fin dall'inizio [...]».

Lett c, d, e

Un piccolo numero di partecipanti[111] suggerisce di sostituire l'elenco dei verbi (leggere, modificare, rimuovere, ecc.) con il verbo «elaborare». Chiedono maggiore precisione, e in particolare una distinzione tra supporti di dati (lettera c) e memoria (lettera d). Secondo ASA è importante determinare se il trattamento si riferisca al supporto di dati o ai dati in esso contenuti. Swimag desidera inoltre maggiore precisione e suggerisce di aggiungere «descrivere e deteriorare» alla lettera c prima di «o rimuovere».

[110] Organizzazioni: ASA, curafutura.

[111] Organizzazioni: ASA, curafutura, santésuisse.

DFS ritiene che affermare nella lettera c che le persone non autorizzate «non possono» non sia sufficiente. Il controllo dei supporti di dati deve «garantire» che le persone non autorizzate non possano leggere, ecc.

ASDPO propone di sostituire «memoria» con «integrità» alla lettera d. Quest'ultimo termine sembra essere più appropriato alla situazione.

Lett. g

La disposizione dovrebbe evitare l'introduzione di nuove notioni non definite nella nLPD o nel rapporto esplicativo; in particolare la nozione di «sistema automatizzato»[112].

La Suva è dell'opinione che dovrebbe essere possibile controllare ogni modifica *a posteriori*.

Secondo Swimag, il sistema automatizzato deve essere in grado di eseguire controlli «in qualsiasi momento». Propone di completare il testo aggiungendo «a quale scopo o in base a quale base legale».

Lett. h

La Suva ritiene che sia sufficiente poter identificare l'organo. Un partecipante[113] aggiunge tuttavia che la verifica dovrebbe essere possibile «in qualsiasi momento».

Lett. i

La Suva ritiene utile sviluppare un piano di salvaguardia. Secondo Swimag, oltre a un incidente fisico o tecnico, bisogna considerare qualsiasi altro pericolo per i dati. Il ripristino deve essere completo, immediato e senza pregiudizi.

Lett. j

Secondo l'Associazione di commercio, questa lettera andrebbe cancellata in quanto irrealistica. Nessuna azienda può garantire la disponibilità dei servizi Cloud in ogni momento, la segnalazione automatica degli errori da parte dei software, ecc.

Qualsiasi malfunzionamento andrebbe segnalato automaticamente dal sistema[114].

Lett. k

L'individuazione deve essere «immediata» e vanno adottati provvedimenti «efficaci e completi»[115].

[112] Organizzazione: Associazione di commercio.

[113] Organizzazione: Swimag.

[114] Organizzazione: suva.

[115] Organizzazione: Swimag.

3.2.3 Art. 3 AP-OLPD: Verbalizzazione

Numerosi partecipanti accolgono la proposta con favore[116]. È considerata molto importante, se non addirittura vista come il futuro fondamento della protezione dei dati in Svizzera[117]. DigiGes sottolinea, inoltre, che questa disposizione poggia su una base legale sufficiente. La verbalizzazione si applica solo al trattamento dei dati a rischio elevato: un'impresa che esegue tale trattamento è obbligata a garantire una protezione elevata. H+ ritiene che un obbligo di verbalizzazione specifico possa essere appropriato (ad esempio per valutare i registri). GL accoglie con favore l'introduzione di «requisiti più rigorosi» al capoverso 2. Quest'obbligo non solo aumenta la fiducia nel trattamento effettuato dagli enti pubblici, ma permette anche un controllo efficace. Inoltre, l'obbligo di verbalizzazione dovrebbe avere un effetto preventivo.

Questo articolo è anche oggetto di molte critiche. La critica principale riguarda la mancanza di una base legale e la necessità di precisione. Secondo diversi partecipanti[118], l'articolo 8 nLPD riguarda la sicurezza dei dati in senso stretto e non funge da base sufficiente per l'obbligo di verbalizzazione. Inoltre, il termine «verbalizzazione» è usato solo nel testo dell'ordinanza e non nella nLPD, a differenza della legge federale del 25 settembre 2015[119] sulle attività informative o della legge federale del 28 giugno 1967[120] sul Controllo delle finanze. Pertanto, la verbalizzazione è vista come uno swiss finish, poiché assente anche nel RGPD. La verbalizzazione crea una considerevole mole supplementare di lavoro. La cancellazione dell'articolo è quindi richiesta, almeno per quanto riguarda il settore privato[121]. Con l'introduzione della valutazione d'impatto relativa alla protezione dei dati (VIPD) e l'uso del registro delle attività di trattamento, la verbalizzazione è considerata un doppione inutile. La verbalizzazione inoltre sarebbe contraria alla volontà del legislatore[122]. H+ afferma anche che una norma generale che richieda la verbalizzazione è sproporzionata.

Diversi partecipanti[123] sottolineano che lo scopo della verbalizzazione, qualora non si possa tecnicamente escludere a priori un trattamento non autorizzato, è quello di permettere di accertare un trattamento non autorizzato *a posteriori*. Così, la valutazione dei rischi e la pianificazione dei provvedimenti costituiscono la base per la necessità di verbalizzazione. Un rischio ipotetico non è sufficiente nè proporzionato. Questo va determinato nel contesto di un'indagine secondo un articolo 1 precedentemente adattato. Bisogna sottolineare che la verbalizzazione è il risultato di misure tecniche e/o organizzative non sufficienti o non efficaci. Il rapporto esplicativo afferma che la verbalizzazione è un mezzo per raggiungere gli obiettivi di cui all'articolo 2. Si chiede inoltre di chiarire se la verbalizzazione debba essere attuata in assenza di

[116] Cantone: GL; partiti: PS; PVS.

[117] Partito: PVS; organizzazione: Anche FRC sottolinea l'importanza del ruolo di questa disposizione per la sicurezza dei dati.

[118] Cantone: ZH; organizzazioni: : ABES, ASA, ASB, ASP, ASPS, Associazione di commercio, ASSL, asut, auto suisse, BNS, CFC, FFS, Coop, Creditreform, curafutura, CURAVIVA.CH, Datenschutzguide.ch, DFS, digitalswitzerland, economiesuisse, EPS, EXPERTsuisse, FSA, FSEP, H+, HKBB, HotellerieSuisse, IGEM, INSOS, IS, la Posta, le banche domestiche, Migros, Raiffeisen, rega, Ringier, santésuisse, Scienceindustries suisse, SDV, senesuisse, SPA, SPITEX suisse, suva, SWICO, Swissholdings, swissICT, Swiss Insights, Swissstaffing, thurbo, UPSA, usam, UTP, UCS, veb.ch, vsi, VUD, Walderwyss. L'ATPrD è del parere che il rimando tra la nLPD e l'ordinanza non è sempre di facile comprensione ed è persino contraddittorio; partito politico: Alleanza del centro.

[119] LAIn, RS 121, cfr. l'art. 78, cpv. 5.

[120] LCF RS 614.0, cfr. l'art. 10, cpv. 3.

[121] Organizzazioni: ASSL, auto suisse, HotellerieSuisse, Swiss Insights, UPSA.

[122] Organizzazioni: ASB, ASP, ASSL, Associazione di commercio, asut, auto suisse, Bär & Karrer, BNS, CFC, FFS, Coop, Creditreform, digitalswitzerland, economiesuisse, EPS, EXPERTsuisse, VSP, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, rega, Ringier, SDV, santésuisse, Scienceindustries suisse, suva, SWICO, Swissholdings, Swiss Insights, thurbo, UPSA, usam, UTP, vsi, VUD, Walderwyss.

[123] Cantoni: AG, AR, BE, GL, GR, NW, VD, ZH; organizzazioni: ASB, FFS, Coop, digitalswitzerland, economiesuisse, FMH, FRC, FSA, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, Raiffeisen, Ringier, santésuisse, Scienceindustries suisse, SDV, suva, thurbo, UPSC, UTP, VUD, Walderwyss.

una valutazione d'impatto sulla protezione dei dati (VIPD). Alcuni partecipanti[124] considerano sufficiente la verbalizzazione qualora non fosse possibile determinare *a posteriori* se i dati sono stati trattati in conformità con gli scopi per cui sono stati collezionati o comunicati (art. 10 cpv. 1 OLPD). Vari partecipanti[125] sottolineano che per rilevare fughe di dati non autorizzate, malware, intrusioni, ecc, la verbalizzazione dell'uso regolare dei dati non è molto utile.

Per alcuni partecipanti[126], conformemente all'articolo 8 nLPD, è prevista un'attuazione della protezione dei dati basata sulle esigenze e in linea con il più attuale stato della tecnica. Tuttavia, ciò è difficile da mettere in pratica; in particolare con una disposizione così dettagliata, che comporta costi di attuazione elevati, è poco chiara e ambigua. Tuttavia, sono dell'opinione che la verbalizzazione sia la soluzione giusta, poiché non vi è altra misura che possa raggiungere lo stesso obiettivo a un costo inferiore. Questa misura, e anche eventuali alternative, dovrebbe come minimo essere espressamente prevista nell'ordinanza. ZH fa notare che la verbalizzazione in caso di rischio elevato è in contraddizione con il rifiuto di stabilire provvedimenti concreti. Secondo un ristretto numero di partecipanti[127], l'obbligo dovrebbe essere limitato ai casi con un rischio (residuo) elevato, ossia quando il provvedimento è conforme all'articolo 1. Di conseguenza, i testi in italiano e francese vanno adattati in tal senso. Il rispetto della disposizione presenta difficoltà pratiche, in particolare a causa delle sanzioni penali (art. 61 lett. c nLPD), che saranno certamente numerose. Alcuni partecipanti[128] fanno notare un rischio di sorveglianza delle persone interessate, giustificato solo se il trattamento presenta un rischio elevato.

Cpv. 1

Si chiede la revisione di questo capoverso. Vari partecipanti[129] affermano che la valutazione d'impatto sulla protezione dei dati (VIPD) non rivela un rischio elevato a causa di un'insufficiente sicurezza dei dati, bensì in considerazione del modo in cui i dati sono trattati. Pertanto, alcuni partecipanti[130] sono dell'opinione che la VIPD non riguardi la sicurezza dei dati.

Secondo diversi partecipanti[131], occorre rinunciare alla verbalizzazione della lettura perché difficilmente realizzabile. Per Swimag è importante aggiungere «così come le finalità o il motivo specifico del trattamento» all'ultima frase.

Alcuni partecipanti[132] si chiedono se la nozione di «trattamento automatizzato» non debba essere definita. Secondo alcuni partecipanti[133], la nozione dovrebbe essere definita *al contrario*, In altre parole, qualsiasi trattamento non manuale è da considerare un trattamento elettronico.

[124] Organizzazioni: ASSL, auto suisse, Bär & Karrer, Swiss Insights, UPSA.

[125] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[126] Organizzazioni: ASPS, CURAVIVA.CH, HÄRTING, INSOS, IS, senesuisse, SPITEX suisse, swissICT.

[127] Organizzazioni: ABES, FFS, Classtime, HDC, la Posta, swissprivacy.law, thurbo, UTP.

[128] Organizzazioni: Creditreform, DigiGes, FRC, vsi.

[129] Organizzazioni: FFS, Coop, EXPERTsuisse, H+, IGEM, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[130] Organizzazioni: FFS, Coop, H+, IGEM, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[131] Organizzazioni: BNS, FFS, curafutura, H+, IGEM, la Posta, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[132] Organizzazioni: Associazione di commercio, BNS, FFS, H+, HDC, IGEM, la Posta, Migros, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[133] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

Cpv. 2

Un certo numero di partecipanti[134] si oppone a un obbligo generale di verbalizzazione per gli organi federali, in quanto contrario al principio di proporzionalità. Per alcuni partecipanti[135], sebbene il rispetto dell'articolo 25 della direttiva (UE) 2016/680 imponga l'elaborazione di una disposizione svizzera, essa dovrebbe essere limitata agli organi federali che vi sono sottoposti. Per il resto andrebbe applicato l'articolo 3 capoverso 1. Alcuni partecipanti[136] sottolineano che l'articolo 57*l* lettera b numero 4 della legge federale del 21 marzo 1997[137] sull'organizzazione del Governo e dell'Amministrazione permette la registrazione dei metadati allo scopo di risalire agli a collezioni di dati, purché la registrazione sia proporzionata. Il fatto che perfino semplici dati personali debbano essere verbalizzati va chiaramente oltre questo requisito. Alcuni partecipanti[138] propongono di includere gli organi federali nel capoverso 1 e di eliminare il capoverso 2. Diversi partecipanti[139] sottolineano inoltre che la verbalizzazione esiste indipendentemente da qualsiasi rischio. Viene effettuata per ogni trattamento automatizzato.

Alcuni partecipanti[140] sono dell'opinione che il regime dovrebbe almeno essere il medesimo per i privati e gli organi federali.

Per Swimag è importante aggiungere «così come le finalità o il motivo specifico del trattamento» all'ultima frase.

Cpv. 3

Poiché non tutti i trattamenti includono una comunicazione, alcuni partecipanti[141] ritengono ragionevole introdurre «se del caso» prima di «sull'identità del destinatario».

Secondo alcuni partecipanti[142], questo capoverso contraddice i due capoversi precedenti. L'idea sembra essere che la verbalizzazione dovrebbe essere utilizzata per evidenziare trattamenti non autorizzati e non violazioni della sicurezza dei dati. Sarebbe opportuno chiarire che il termine «destinatario» si riferisce all'organizzazione e non all'individuo.

Secondo l'opinione di due partecipanti[143], la verbalizzazione è una documentazione qualificata che porta alla profilazione. È possibile stabilire chi ha trattato i dati, quando, come e in che misura. Si tratta di un trattamento qualificato e automatizzato dei dati della persona che ha trattato i dati. Una base legale in senso formale è quindi indispensabile, soprattutto se nel contesto professionale la verbalizzazione dovesse permettere una vera e propria profilazione e il monitoraggio del comportamento del dipendente.

---

[134] Cantoni: GR, NW, SH, SO, VD; organizzazioni: FFS, curafutura, HDC, IGEM, la Posta, Incaricato cantonale della protezione dei dati SZ, OW e NW, privatim, Ringier, santésuisse, suva, swissICT, thurbo, UTP, VUD.

[135] Cantone: SH; organizzazioni: FFS, curafutura, HDC, la Posta, thurbo, UTP.

[136] Cantoni: AR, ATPrD, BE, GL, NW ; organizzazioni: Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[137] LOGA, RS 172.010.

[138] Cantoni: AR, BE, GL, NW, SO; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[139] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[140] Organizzazioni: ASDPO, swissICT.

[141] Cantoni: AG, AR, BE, GL, NW, VD; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[142] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[143] Organizzazioni: Creditreform, VSI.

Cpv. 4

Alcuni partecipanti[144] sono a favore del mantenimento dell'attuale durata di conservazione di un anno. Sono dell'opinione che il § 5 dell'ordinanza sulla legge sull'informazione, la protezione dei dati e sui registri del Cantone di Argovia dovrebbe essere preso come modello[145]. Per molti partecipanti[146], la sfida dei crescenti attacchi informatici contraddice qualsiasi estensione della durata di conservazione. Anziché permettere una migliore valutazione, questa estensione genererebbe inutilmente costi e sforzi supplementari senza raggiungere un livello di protezione più alto. La conservazione separata non porterebbe a un risultato migliore. Una maggiore protezione contro i cambiamenti successivi sarebbe più idonea. Condurre una tale procedura di separazione comporta anche un rischio per la sicurezza dei dati. La durata di conservazione andrebbe concepita come una durata minima appropriata e non in forma rigida. Una durata di due anni è considerata inappropriata. ZH afferma che una durata di conservazione di alcuni giorni o mesi è la sola appropriata. economiesuisse è del parere che la durata di conservazione dovrebbe dipendere dalla durata del trattamento. Due partecipanti[147] sono, al contrario, soddisfatti e sono a favore della durata di conservazione di due anni. Alcuni partecipanti[148] ritengono che questo obbligo porti allo sviluppo di grandi raccolte di dati con lunghi periodi di conservazione (ad esempio i dati degli utenti/collaboratori, ecc.). Alcuni partecipanti[149] propongono di revocare la conservazione separata.

Diversi partecipanti[150] sottolineano che per gli organi federali, l'articolo 57*m* segg. LOGA e la sua ordinanza sull'organizzazione del Governo e dell'Amministrazione[151] definiscono la procedura. Una valutazione personale non sempre è necessaria. All'ultima frase di questo capoverso andrebbe aggiunto quanto segue: «Sono utilizzati solo a questo scopo e per uso personale nella misura ove ciò sia necessario». La limitazione dell'accesso e quella dello scopo sono considerate troppo severe. Altre ragioni potrebbero giustificare la consultazione dei registri, in particolare da parte di un titololare o di un responsabile del trattamento. Occorre eliminare i doppioni. La disposizione dovrebbe prevedere una riserva per le deroghe contenute nella legislazione speciale. Il capoverso andrebbe eliminato, o la cerchia delle persone che hanno accesso andrebbe ampliata.

Alcuni partecipanti[152] ritengono che la formulazione «separatamente dal sistema in cui sono trattati i dati personali» andrebbe sostituita da «in modo sicuro».

---

144 Cantone: GL; organizzazioni: asut, curafutura, Sunrise UPC, SWICO, swissICT.

145 VIDAG, SAR 150.711.

146 Cantoni: GL, TG, ZH; organizzazioni: ASDPO, ASP, ASPS, Associazione di commercio, ASSL, asut, auto suisse, Bär & Karrer, FFS, Creditreform, curafutura, CURAVIVA.CH, EPS, FMH, VSP, H+, INSOS, IS, la Posta, rega, Ringier, senesuisse, SPITEXsuisse, SSO, Sunrise UPC, suva, SWICO, Swimag, Swiss Insights, thurbo, UPSA, usam, UTP, veb.ch, vsi, VUD, Walderwyss. ASDPO e Bär & Karrer propongono di armonizzare tutte le durate presenti nell'ordinanza. Swimag propone una durata generale di cinque anni.

147 Partito: PS; organizzazione: USS.

148 Cantoni: BL, ZH. Secondo BL, è l'obbligo generale di verbalizzazione che porta alla creazione di grandi banche dati.

149 Cantoni: TG, ZH; organizzazioni: Associazione di commercio., ASSL, auto suisse, Classtime, FFS, Creditreform, H+, la Posta, Migros, rega, Ringier, SPA, suva, Swiss Insights, thurbo, UPSA, UTP, vsi, VUD, Walderwyss.

150 Cantoni: AG, AR, BE, GL, NW, SH, VD; organizzazioni: ATPrD, Migros, Incaricato cantonale della protezione dei dati SZ, OW e NW., Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, UCS, VUD.

151 OLOGA, RS 172.010.1.

152 Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

3.2.4 Art. 4 AP-OLPD: Regolamento dei privati sul trattamento

Diversi partecipanti[153] accolgono espressamente con favore questa disposizione, che è vista come una pietra miliare per il futuro della legislazione sulla protezione dei dati. Altri partecipanti[154] vorrebbero addirittura estenderne la portata, poiché considerano arbitrati i criteri del capoverso 1 e ritengono che non coprano tutti i trattamenti critici. Il provvedimento è quindi accettato, ma si richiedono alcune precisazioni. È considerata una misura che promuove la minimizzazione dei dati[155] e si ritiene giustificato che vengano fissati requisiti più elevati per i trattamenti a rischio elevato, come il trattamento dei dati sensibili o la profilazione[156].

Molti altri partecipanti[157] ritengono invece la disposizione contraria alla volontà del legislatore e ridondante. Secondo il parere di molti partecipanti[158], per quanto riguarda l'obbligo di documentazione, si è deciso di limitarlo al registro delle attività di trattamento o alla valutazione d'impatto sulla protezione dei dati (VIPD). I pareri critici sottolineano l'assenza di una base legale. Quindi, il regolamento sul trattamento non serve a garantire la sicurezza dei dati in senso stretto (disciplinata dall'art. 8 nLPD), ma assicura il rispetto dei principi e delle prescrizioni sulla protezione dei dati. I suddetti partecipanti fanno notare che il RGPD non ne fa menzione, anche se ne deriva l'obbligo di documentazione. Criticano questo swiss finish. Si chiede la cancellazione di questa disposizione. Diversi partecipanti[159] sono dell'opinione che quest'obbligo contraddica l'approccio basato sui rischi. Alcuni partecipanti[160] ricordano che l'articolo 11*a* LPD non è stato ripreso deliberatamente, come spiegato nel rapporto esplicativo.

Per diversi partecipanti[161], il quadro giuridico è il seguente: l'articolo 36 LPD offre la possibilità di redigere un «regolamento sul trattamento», mentre l'articolo 12 nLPD introduce la nozione di «registro delle attività di trattamento». Ritengono che il sistema sembra aver sostituito il regolamento con il registro. Si sottolinea che gli articoli 1 e 2 non menzionano tra i provvedimenti il regolamento sul trattamento. Il valore aggiunto di questo strumento in termini di trasparenza è discutibile; ancor più con l'introduzione del registro delle attività di trattamento. Così come la verbalizzazione dei diritti di accesso o degli accessi, i provvedimenti tecnici o organizzativi rappresentano degli obblighi. Tuttavia, restano necessari ulteriori chiarimenti per evitare inutili doppioni e una mole di lavoro aggiuntivo non indispensabile. Alcuni partecipanti[162] affermano che il regolamento sul trattamento è inutile e, al contrario, creerebbe addirittura un rischio per il titolare se le persone interessate cercassero di ottenerlo tramite il diritto di accesso. In effetti, alcune delle informazioni contenute nel regolamento rientrano nell'obbligo di informare.

---

153 Partiti: PS, PVS; organizzazione: DigiGes.

154 Cantoni: AG, AR, BE, GL, GR, NW, SH, SO, SZ, UR, VD, ZH; partito: PVS; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

155 Partito: PS.

156 Organizzazione: DigiGes.

157 Organizzazioni: ASA, ASB, asut, BNS, FFS, curafutura, DFS, economiesuisse, EXPERTsuisse, forum PMI, H+, HKBB, IGEM, la Posta, le banche domestiche, proFonds, santésuisse, Scienceindustries suisse, SDV, Sunrise UPC, suva, SWICO, swissICT, thurbo, UBCS, UTP, VUD, Walderwyss.

158 Cantoni: AR, BE, GL, GE, TG; organizzazioni: ASB, ASA, ASDPO, ASSL, asut, ATPrD, auto suisse, BNS, FFS, Coop, Creditreform, curaturura, DFS, digitalswitzerland, economiesuisse, EXPERT suisse, H+, HÄRTING, HDC, HKBB, HotellerieSuisse, IGEM, la Posta, le banche domestiche, Migros, pharmasuisse, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, proFonds, Raiffeisen, rega, Ringier, Scienceindustries suisse, SDV, SSO, Sunrise, UPC, suva, SWICO, swissICT, SwissHoldings, Swiss Insights, Swissstaffing, thurbo, UPSA, UTP, vsi, VUD, Walderwyss. privatim in particolare chiede l'eliminazione del capoverso 3. Su questo argomento, cfr. nbp n. 176; partito: PLR.

159 Organizzazioni: ASSL, auto suisse, Raiffeisen, Swiss Insights, UPSA.

160 Organizzazioni: HotellerieSuisse, proFonds, Raiffeisen.

161 Partito: PLR; organizzazioni: ASB, ASA, asut, Bär & Karrer, BNS, FFS, curafutura, digitalswitzerland, economiesuisse, H+, HDC, HKBB, HotellerieSuisse, la Posta, le banche domestiche Migros, Raiffeisen, rega, Ringier, santésuisse, Scienceindustries suisse, SDV, suisa, Sunrise UPC, suva, SWICO, SwissHoldings, thurbo, UTP, veb.ch, VUD, Walderwyss.

162 Organizzazioni: ASA, FFS, Coop, curafutura, H+, IGEM, Migros, Raiffeisen, rega, Ringier, suva, suiva, thurbo, UTP, VUD e Walderwyss ritengono che alcuni sarebbero tentati di ottenere il regolamento tramite la richiesta di accesso.

Due partecipanti[163] sono dell'opinione che, come minimo, il campo d'applicazione e la necessità andrebbero precisati, in particolare per le imprese individuali.

Diversi partecipanti[164] ritengono utile ricordare che l'obbligo di emanare un regolamento sul trattamento non è nuovo e figura nel testo attuale dell'ordinanza. Affermano che, vista la scelta di limitare l'obbligo di documentazione e d'informazione (VIPD, registro delle attività di trattamento o dichiarazione di confidenzialità), ci si sarebbe attesa la sua eliminazione nella nuova ordinanza.

Cpv. 1

Limitare il regolamento sul trattamento ai dati sensibili su larga scala o alla profilazione a rischio elevato è per molti partecipanti[165] arbitrario o addirittura troppo limitato. L'approccio basato sui rischi, come nell'articolo 22 capoverso 1 nLPD, non giustifica tale ragionamento. Le lettere a e b vanno intese come esempi non esaustivi che presentano sempre un rischio elavato. Questa restrizione (lett. a e b) non permette di contemplare il trattamento dei dati che sono critici per i diritti della personalità. Si propone quindi di riprendere i requisiti della valutazione d'impatto sulla protezione dei dati (VIPD) (art. 22, cpv. 1 nLPD). Nel contesto della VIPD vengono prodotti molti documenti (art. 22, cpv. 3 nLPD). Questi possono far parte del regolamento del trattamento. Vari partecipanti[166] fanno notare che secondo il capoverso 2 le informazioni essenziali sono già in ogni caso documentate nella VIPD e il resto nell'inventario che va comunque creato. Certi[167] mettono quindi in dubbio il valore aggiunto di un tale regolamento.

Secondo vari partecipanti[168], anche se la probabilità che nella prassi siano allestiti regolamenti sul trattamento per la «profilazione a rischio elevato» è molto bassa, si pone la questione del momento dal quale i dati sono considerati trattati «su vasta scala». Nelle risorse umane, la nozione sarebbe giustificata in caso di volumi di dati di media o grande dimensione; mentre in termini di banche dati bibliografiche sembrerebbe di no. Questo vale anche per le imprese dei media che pubblicano articoli su politica e società, poiché si tratta di dati personali sensibili (opinioni politiche, ecc.). Bisogna riconoscere la necessità di un chiarimento nella pratica (ambito medico, ecc.). Swimag propone di eliminare «su vasta scala». A suo parere, è proprio nel caso di trattamenti minori e isolati di dati personali sensibili che la sensibilizzazione è necessaria; da qui la necessità di stabilire un pertinente regolamento sul trattamento. Suggerisce anche di attenersi alla profilazione semplice, anziché alla «profilazione a rischio elevato». Secondo Bär&Karrer le imprese si sono abituate a stabilire direttive interne. Tuttavia, non sono così dettagliate come proposto nell'articolo 4. Ciononostante, nella pratica è poco concepibile la redazione di un tale regolamento per i processi di trattamento automatizzato di dati soggetti a cambiamenti costanti e quindi regolarmente adattati o estesi. Alcuni partecipanti[169] sottolineano inoltre che il trattamento di dati particolarmente sensibili può richiedere una regolamen-

[163] Organizzazioni: Creditreform, vsi.

[164] Organizzazioni: ASSL, auto suisse, FFS, Coop, H+, la Posta, Migros, Ringier, suva, Swiss Insights, thurbo, UPSA, UTP, VUD. Ad eccezione di Coop, fanno notare che, per quanto riguarda la verbalizzazione (art. 3), l'obbligo di documentare è stato abolito in favore dell'obbligo di tenere un registro delle attività di trattamento.

[165] Cantoni: AG, AR, BE, GL, GR, NW, SH, SO, SZ, UR, VD, ZH; partiti: PVS; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[166] Organizzazioni: FFS, H+, la Posta, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[167] Cantone: BE; organizzazioni: ASA, ASSL, auto Suisse, curafutura, rega, Swiss Insights, UPSA, vsi.

[168] Organizzazioni: ASB, Bibliosuisse, FFS, Coop, economiesuisse, ETH-Bibliothek, FMH, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, suva, thurbo, UTP, VUD, Walderwyss.

[169] Organizzazioni: FFS, Coop, H+, IGEM, la Posta, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

tazione interna. Tuttavia, questo aspetto è già sufficientemente disciplinato dall'articolo 7 capoverso 1 nLPD. Alcuni partecipanti[170] sollevano la questione dell'ampio margine di interpretazione dell'espressione «rischio elevato». Raccomandano di fornire maggiori informazioni nel rapporto esplicativo.

Secondo swissICT, poiché il regolamento sul trattamento è una misura organizzativa e tecnica per garantire la sicurezza dei dati (in linea con il principio della *privacy by design* e *by default*), sono presenti errori nei criteri di esclusione. I rischi elevati per la personalità si mescolano agli aspetti di sicurezza dei dati (confidenzialità, integrità, disponibilità). La struttura di questo capoverso va ripensata.

Cpv. 2

Il capoverso trarrebbe beneficio da un riferimento alle norme sulla tecnologia dell'informazione. Quantomeno, sarebbe opportuno un riferimento alle disposizioni specifiche sulla protezione dei dati (lett. h, j)[171]. ZH aggiunge che in presenza di una certificazione (per esempio: ISO 270001), è giustificato rinunciare a un regolamento sul trattamento separato.

Vari partecipanti[172] sottolineano che le lettere a, b, c ed f fanno parte delle informazioni che andrebbero incluse nel registro delle attività di trattamento. Le altre lettere andrebbero prese in considerazione nella valutazione dell'impatto sulla protezione dei dati (VIPD) se rilevanti per la valutazione dei rischi o come misura di riduzione dei rischi. Questi punti sono pertanto già documentati. Non si tratta solo di una questione di sicurezza dei dati, ma di rispetto della legislazione sulla protezione dei dati.

Secondo alcuni partecipanti[173], andrebbe precisato che le indicazioni di questo capoverso vanno fornite solo in relazione ai trattamenti che rientrano nell'articolo 1 capoverso 1 lettere a e/o b.

Diversi partecipanti[174] chiedono di ridurre l'elenco, poiché i requisiti per il trattamento dei dati sensibili sono troppo onerosi, soprattutto per le organizzazioni del settore medico. Le lettere d, e, j andrebbero eliminate in quanto creano un onere amministrativo non indispensabile. Andrebbe invece adeguata la lettera i poiché troppo dettagliata. Le lettere a, b, c, f e g sono accolte con favore come provvedimenti di centrale importanza per garantire la sicurezza dei dati. Sono ritenute sufficienti a garantire il rispetto della protezione dei dati. Anche la lettera h è accolta favorevolmente. Il PS considera essenziale il principio di minimizzazione dei dati. Accoglie quindi con favore la lettera h.

Due partecipanti[175] chiedono di essere esplicitamente esclusi dal campo d'applicazione.

[170] Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, SDV, Scienceindustries suisse.

[171] Cantoni: BE, GL, VD, ZH; organizzazione: ATPrD, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[172] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, suva, thurbo, UTP, VUD, Walderwyss.

[173] Organizzazioni: ASSL, auto Suisse, Swiss Insights, UPSA.

[174] Organizzazioni: ASPS, CURAVIVA suisse, INSOS suisse, IS, senesuisse, SPITEX suisse.

[175] Organizzazioni: Bibliosuisse, Biblioteca dell'ETH.

Cpv. 3

Numerosi partecipanti[176] ritengono che questo capoverso non tenga conto della prassi. Il consulente per la protezione dei dati deve essere uno specialista. Il regolamento sul trattamento è quindi redatto insieme al consulente e non messo a sua disposizione in una forma a lui comprensibile. Uno dei suoi compiti è quello di partecipare all'attuazione delle norme sulla protezione dei dati (art. 10 cpv. 2 lett. b nLPD). Inoltre, il consulente per la protezione dei dati deve possedere le conoscenze professionali necessarie (art. 10 cpv. 3 lett. c nLPD). L'espressione «in una forma a lui comprensibile» sembra disconoscere quanto sopracitato e va quindi eliminata.

Diversi partecipanti[177] notano che il regolamento non andrebbe pubblicato né annunciato all'IFPDT. L'introduzione della presentazione al consulente per la protezione dei dati è pertanto contraddittoria. Dal punto di vista legale non vi è alcun obbligo di istituire questa pratica. La seconda metà della frase andrebbe quindi eliminata. SO propone, ad esempio, che il rapporto esplicativo specifichi che la designazione di un consulente per la protezione dei dati è facoltativa.

Due partecipanti[178] sono dell'opinione che l'avverbio «regolarmente» crei un inutile onere burocratico o porti addirittura al mancato rispetto della regola. L'aggiornamento andrebbe eseguito solo al bisogno. Altri partecipanti[179] sottolineano che, come nell'articolo 1 capoverso 2, gli intervalli tra gli aggiornamenti andrebbero indicati con maggiore precisione, così da evitare il rischio di incertezza giuridica e di controversie. Si propone di utilizzare la seguente espressione: «almeno una volta l'anno».

Swimag è del parere che il tenore della disposizione dovrebbe riferirsi al titolare e al responsabile e non al privato.

3.2.5 Art. 5 AP-OLPD: Regolamento per il trattamento dei dati degli organi federali

Poiché gli articoli 4 e 5 trattano il regolamento sul trattamento, molti partecipanti[180] ritengono opportuno fare riferimento alle osservazioni relative all'articolo 4. Si sottolinea semplicemente che il regolamento è sproporzionato e non ha una base legale. Inoltre, il regolamento sul trattamento costituisce in parte una copia del registro delle attività di trattamento e della valutazione d'impatto sulla protezione dei dati (VIPD). Si chiede la cancellazione di questa disposizione. Due partecipanti[181] sottolineano che un'eventuale eliminazione dell'articolo 5 richiederebbe, come minimo, un adattamento dell'articolo 84*b* della legge federale del 18 marzo 1994[182] sull'assicurazione malattie.

---

[176] Cantoni: AR, BE, GL, NW, SH, SO, TG, UR, VD, ZH; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[177] Organizzazioni: FFS, H+, Hotelleriesuisse, IGEM, la Posta, Migros, Ringier, santésuisse, suva, thurbo, UTP, VUD, Walderwyss.

[178] Organizzazioni: Creditreform, vsi.

[179] Organizzazioni: ASPS, CURAVIVA suisse, INSOS suisse, IS, senesuisse, SPITEX suisse.

[180] Cantoni: AR, GL, NW, SH, SO, SZ, VD, ZH. BE propone sia l'eliminazione dell'articolo 4 che dell'articolo 5; organizzazioni: ASA, ASDPO, asut, ATPrD, FFS, curaturura, Datenschutzguide.ch, DFS, H+, HÄRTING, HDC, IGEM, la Posta, Migros, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, Ringier, santésuisse, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, VUD, Walderwyss.

[181] Organizzazioni: curafutura, santésuisse.

[182] LAMal, RS 832.10.

Alcuni partecipanti[183] sottolineano che il campo d'applicazione della disposizione è troppo ampia per gli organi federali. La Posta precisa che l'obbligo di regolamentare l'intera profilazione senza rischi elevati richiede in ogni caso una base legale per gli organi federali (art. 34 cpv. 2 lett. b nLPD). Sulla base della valutazione dei rischi effettuata dal legislatore, possono essere stabiliti obblighi normativi specifici nella legislazione settoriale. Due partecipanti[184] sottolineano che una burocrazia eccessiva aumenta lo spreco di risorse (personale, fondi), soprattutto per gli organi federali. Questo commento si applica in generale all'intero progetto.

Cpv. 1 lett. b

Poiché il concetto è molto ampio, BE ritiene che la profilazione andrebbe almeno intesa, per analogia, entro i limiti dell'articolo 4 capoverso 1 lettera b.

Cpv. 2

Alcuni partecipanti[185] chiedono maggiore chiarezza. La formulazione suggerisce che il regolamento potrebbe contenere più indicazioni.

3.2.6 Art. 6 AP-OLPD: Modalità

La disposizione è accolta con favore e considerata essenziale[186], ma è anche fortemente criticata. Se ne richiede la cancellazione, almeno di alcuni capoversi o alcune frasi. In generale, si chiede un adeguamento del testo[187]. Un gran numero di partecipanti[188] critica la mancanza di una base legale. Secondo l'articolo 9 capoverso 1 lettera a nLPD, il titolare del trattamento deve assicurarsi che vengano eseguiti solo i trattamenti che egli stesso è autorizzato a fare. L'obbligo del titolare del trattamento di «assicurarsi» che il trattamento effettuato dal responsabile sia conforme al contratto e alla legge non può essere continuo (art. 6 cpv. 1 secondo periodo e art. 6 cpv. 2 secondo periodo). Questa ripetizione nell'ordinanza è ingiustificata, sproporzionata e non rientra nel quadro della delega al Consiglio federale. La nLPD sancisce solo che l'ente pubblico o il privato sono responsabili della protezione dei dati. Il titolare del trattamento deve, come minimo, assicurare per contratto che sia garantita una protezione dei dati equivalente. Non può garantire, ma solo «controllare» (art. 9, capoverso 2, nLPD). Il verbo «assicurare» andrebbe adattato o sostituito da «controllare che» o «controllare adeguatamente». Si propone la seguente formulazione: «Conformemente all'articolo 9 capoverso 1 lettera a nLPD il titolare del trattamento deve controllare che sia rispettata la LPD». SZ ritiene che questo equivarrebbe a un controllo permanente. Questo modo di procedere non costituisce il senso e lo scopo dell'esternalizzazione delle attività amministrative. Il titolare del trattamento dei dati è chiaramente corresponsabile del trattamento dei dati conformemente al mandato e alla legge.

Alcuni partecipanti[189] non comprendono la ragione di estendere il campo di applicazione ai privati, poiché questo aspetto è già coperto dall'articolo 9. Fanno notare che l'articolo 6 capoversi 1 e 2 è modellato sull'articolo 22 OLPD, che si applica solo agli organi federali. Quando

[183] Organizzazioni: asut, BNS, FFS, H+, IGEM, la Posta, Migros, Ringier, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, Walderwyss, VUD.

[184] Organizzazioni: Creditreform, vsi.

[185] Organizzazioni: FFS, H+, IGEM, la Posta, Migros, Ringier, suva, VUD, Walderwyss.

[186] Organizzazione: DigiGes.

[187] Cantone: SZ; organizzazioni: ASB, ASDPO, ASP, ASSL, Associazione di commercio, asut, Bär & Karrer, BNS, Creditreform, DFS, EPS, FER, FSA, VSP, GastroSuisse, Härting, IGEM, la Posta, Raiffeisen, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, swissICT, Swiss Insights, Swissstaffing, UPSA, usam, vsi, VUD, Walderwyss.

[188] Cantone: SZ; organizzazioni: ASB, ASP, ASSL, Associazione di commercio, asut, BNS, FFS, Creditreform, DFS, EPS, FER, FMH, VSP, GastroSuisse, H+, HÄRTING, HotellerieSuisse, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, swissICT, Swiss Insights, Swissstaffing, swissICT, thurbo, UPSA, usam, UTP, vsi, VUD, Walderwyss.

[189] Organizzazioni: Bär & Karrer, swissICT.

un titolare esternalizza il trattamento a un responsabile all'estero, la LDP non si applica al responsabile. Va da sé che il titolare deve rispettare le regole di cui agli articoli 16-18 nLDP. Il caso di applicazione in cui un responsabile estero tratta dati che non gli sono stati precedentemente trasmessi dalla Svizzera andrebbe disciplinato nell'articolo 16 nLPD e non nel contesto dell'articolo 6, capoverso 2.

Cpv. 1

TG accoglie con favore il fatto che un mandatario a cui ci si rivolge deve garantire una protezione dei dati equivalente. Anche DigiGes accoglie con favore questo capoverso.

Alcuni partecipanti[190] si dispiacciono della falsa impressione data dalla prima frase, secondo cui la responsabilità del titolare non è limitata in alcun modo. È importante spiegare cosa si intende per «titolare della protezione dei dati». Nel caso in cui si intenda la responsabilità civile, questa responsabilità causale non è prevista dal legislatore. Questo andrebbe anche oltre l'articolo 82 paragrafo 3 RGPD. Senza dimenticare che l'articolo 41 del Codice delle obbligazioni[191] resta applicabile alla responsabilità civile.

Per quanto riguarda il secondo periodo, Curafutura mette in dubbio la necessità di sostituire «conformemente al contratto» con «conformemente al contratto o alla legge». Insieme ad altri partecipanti[192], spiega che il titolare non può garantire che il trattamento sia conforme al contratto e alla legge. Può solo cercare di provvedere affinché lo sia, come previsto dall'articolo 28 paragrafo 1 RGPD. In effetti, non appena i dati sono affidati a un responsabile del trattamento, la garanzia della sicurezza dei dati non è più nella sfera d'influenza del o dei titolari del trattamento, oppure la loro influenza è fortemente limitata. Tra le formulazioni, si propone la seguente: «Il titolare del trattamento che affida a un responsabile il trattamento di dati personali rimane responsabile della protezione dei dati. Egli controlla che i dati siano trattati in conformità al contratto o alla legge». Come minimo, i titolari dovrebbero essere tenuti a fare ricorso solo a responsabili che adottino provvedimenti adeguati. Le spiegazioni fornite in relazione all'articolo 22 paragrafo 3 della direttiva (UE) 2016/680 non forniscono ulteriore chiarezza all'articolo 6. Analogamente all'articolo 28 paragrafo 3 RGPD sarebbe consigliabile aggiungere all'articolo 6 il contenuto minimo obbligatorio da includere nei contratti per i responsabili del trattamento: l'oggetto, la durata, la natura e lo scopo del trattamento dei dati, il tipo di dati personali, le categorie di interessati nonché gli obblighi e i diritti del titolare del trattamento. Secondo proFonds, è sufficiente che il titolare vincoli contrattualmente il responsabile agli obblighi legali e lo induca così a trattare i dati in conformità con la legge. Le organizzazioni e le associazioni di piccole e medie dimensioni generalmente non hanno né la possibilità né le risorse per effettuare un controllo completo. Sarebbe pertanto opportuno aggiungere che il titolare deve organizzare contrattualmente i mandati in modo tale che siano conformi alla legge.

FSA si chiede cosa s'intenda per trattamento conforme al contratto o alla legge, poiché ritiene che la questione è già contemplata dall'articolo 9 capoverso 1 nLPD d. Bär & Karrer propone di eliminare «al contratto o». Il PPS lamenta la mancanza di una definizione chiara di ciò che si intende per «assicurare un trattamento almeno conforme al contratto o alla legge».

Secondo TG, la formulazione secondo cui la protezione dei dati va assicurata per contratto se la legge straniera viola la protezione dei dati in Svizzera andrebbe corretta. Cita come esempi

[190] Organizzazioni: ASB, asut, BNS, FFS, H+, IGEM, la Posta, le banche domestiche, Migros, Ringier, SPA, suisa, Sunrise UPC, suva, SWICO, swissICT, thurbo, UTP, VUD, Walderwyss.

[191] CO, RS 220.

[192] Organizzazioni: ASA, ASSL, auto suisse, CFC, curafutura, FER, Gastrosuisse, HotellerieSuisse, santésuisse, SG, SSO, Swiss Insights, UPSA.

la legge cinese sull'intelligence nazionale e la legislazione statunitense. Queste leggi richiedono ai fornitori che hanno un legame con il loro Paese di rivelare alle autorità straniere qualsiasi comunicazione (elettronica), registrazioni o altre informazioni, comprese quelle situate al di fuori dei loro confini. Qualsiasi obbligo contrattuale contrario a queste disposizioni cinesi o americane avrebbe poche probabilità di essere rispettato.

Cpv. 2

Secondo alcuni partecipanti[193], in virtù dell'articolo 3 nLPD, è improbabile che un responsabile non sia soggetto alla LPD. Avrebbe senso eliminare questo capoverso.

Due partecipanti[194] ritengono applicabile l'elenco dei Paesi dell'allegato 1 della nLPD.

Diversi partecipanti[195] dichiarano che il significato e lo scopo del capoverso non sono chiari. Il contenuto è già contemplato dagli articoli 16 e 17 nLPD. In questo senso, il rapporto esplicativo menziona che l'articolo 6 capoverso 2 corrisponde all'attuale articolo 22 capoverso 3 OLPD. L'unica differenza è che la disposizione si applica solo agli organi federali, mentre l'articolo 6 capoverso 2 si applica al trattamento sia da parte di privati sia da parte degli organi federali. Non vi è una spiegazione per questa delimitazione. La disposizione sembra avere senso in casi speciali, come quando un titolare del trattamento svizzero chiede a un responsabile straniero di trattare i dati senza comunicazione dalla Svizzera e l'articolo 16 nLPD non è applicabile. Da un punto di vista sistematico, tuttavia, questo caso andrebbe regolato nell'articolo 16 nLPD e non nell'ordinanza. Giuridicamente, la base legale corretta è l'articolo 9 capoverso 1 lettera a nLPD. In caso di trattamento su mandato, bisogna garantire che i dati siano trattati solo nel modo in cui il titolare del trattamento è autorizzato a farlo, il che è previsto dall'articolo 9 capoverso 1 lettera a nLPD. È probabile che la regola esistente sia semplicemente stata ripresa. È quindi difficile capire perché questo capoverso sia necessario e quale sia la sua base legale.

Alcuni partecipanti[196] chiedono l'eliminazione di questo capoverso adducendo che la comunicazione all'estero è già prevista in un'altra disposizione (art. 8). Inoltre, non si può pretendere che il titolare del trattamento conosca l'intera legislazione pertinente. Se si mantenesse questo disciplinamento, il suggerimento è quello di chiarire che «in assenza di un tale disciplinamento, va garantita un'adeguata protezione dei dati». In questo senso, sarebbe opportuno menzionare che se il responsabile non è soggetto alla LPD, il titolare deve assicurarsi che altre disposizioni legali garantiscano una protezione dei dati equivalente. In caso contrario, deve garantire tale protezione per via contrattuale secondo l'articolo 16 capoverso 2 nLPD. Tuttavia, sarebbe preferibile eliminare questo capoverso.

Secondo il PPS, come la nLPD, l'articolo 6 capoverso 2 è superato non solo alla luce della recente giurisprudenza (ad esempio la sentenza Schrems II della Corte di giustizia dell'UE), ma anche alla luce del diritto europeo (accesso al mercato unico digitale dell'UE). Poiché le clausole contrattuali standard da sole non sono sufficienti, propone di cancellare questo capoverso o la seconda frase e di sostituirla con un rinvio alle direttive dell'IFPDT.

[193] Organizzazioni: ASDPO, HDC, swissprivacy.law.

[194] Organizzazioni: ASA, curafutura.

[195] Organizzazioni: ASB, FFS, digitalswitzerland, economiesuisse, EXPERT suisse, H+, HÄRTING, HKBB, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, suva, Swissstaffing, thurbo, UTP, VUD, Walderwyss.

[196] Organizzazioni: ASPS, ASSL, auto suisse, CURAVIVA Suisse, FSA, INSOS, IS, senesuisse, SPA, SPITEX suisse, Swiss Insights, UPSA, usam.

Cpv. 3

Mentre alcuni partecipanti[197] s'interrogano sull'attualità della «forma scritta», altri due partecipanti[198] hanno accolto con favore l'uso di questa forma per l'autorizzazione della delega di secondo livello. Tuttavia, essi osservano che questo requisito non è menzionato nella nLPD. Ci si chiede quindi se questo possa davvero essere imposto agli organi federali che non sono soggetti alla direttiva 2016/680, dato che l'articolo 22 paragrafo 2 della direttiva 2016/680 menziona il consenso scritto nel settore pubblico. Secondo la suva, l'autorizzazione scritta degli organi federali corrisponde allo standard del RGPD. Tuttavia, l'articolo 9 capoverso 3 nLPD non prevede la forma scritta. L'ASDPO ritiene che l'accordo scritto dovrebbe applicarsi anche al titolare privato. Curafutura aggiunge che, poiché la tecnologia digitale diventa sempre più importante, sarebbe opportuno offrire un'alternativa alla forma scritta. La nuova versione della legge federale sul contratto d'assicurazione[199], entrata in vigore nel gennaio 2022, dovrebbe essere presa come modello. Essa introduce la forma scritta o «un'altra forma che consenta la prova per testo». Pertanto, alcuni partecipanti[200] propongono di riprendere quest'ultima formulazione sul modello dell'articolo 28 paragrafo 2 RGPD, che con l'espressione «per iscritto» comprende la forma elettronica qualsiasi altra forma che consenta la prova per testo. Si propone la seguente formulazione: «per scritto, in forma elettronica o in un'altra forma che consenta la prova per testo». BE ritiene che la forma scritta andrebbe sostituita da «un'altra forma di testo inalterabile». Inoltre, il rapporto esplicativo dovrebbe precisare che la forma scritta indica in particolare documenti in forma cartacea o elettronica. LU suggerisce di menzionare espressamente la forma elettronica usando espressioni come «consenso esplicito», «fissare in forma di testo» o «registrare». Sarebbe comunque appropriato eliminare i requisiti di forma. Santésuisse sottolinea che il requisito della forma scritta non dovrebbe rappresentare un ostacolo.

Curafutura è del parere che una riserva che permetta di opporsi dovrebbe sostituire l'approvazione. BE propone di specificare «solo con la previa approvazione dell'organo federale». Alcuni partecipanti[201] sottolineano che un'autorizzazione generale conformemente al RGPD è sufficiente. Un'autorizzazione scritta specifica per ciascun caso non è quindi necessaria. Citano l'esempio dei servizi online standard, che non prevedono questa possibilità nelle loro condizioni generali. Non sarebbe quindi più possibile ottenere tali servizi.

VD nota un refuso nel testo francese: «Lorsque le responsable de traitement…» dovrebbe essere corretto in «Lorsque le responsable du traitement…».

3.2.7 Art. 7 AP-OLPD: Informazione del consulente per la protezione dei dati dell'organo federale

La disposizione è considerata superflua e se ne chiede la cancellazione[202]. Alcuni partecipanti[203] sottolineano che, conformemente all'articolo 28 AP-OLPD e all'articolo 10 capoverso 2 lettera b nLPD, il consulente per la protezione dei dati dell'organo federale è in ogni caso

[197] Organizzazioni: Creditreform, vsi.

[198] Organizzazioni: HDC, swissprivacy.law.

[199] LCA, RS 221.229.1.

[200] Cantone: LU; organizzazioni: ASSL, asut, auto suisse, FFS, Creditreform, Datenschutzguide.ch, DFS, H+, HDC, IGEM, la Posta, Migros, Ringier, SPA, Sunrise UPC, suva, SWICO, swissICT, Swiss Insights, thurbo, UTP, VUD, Walderwyss.

[201] Organizzazioni: CFF, thurbo, UTP.

[202] Cantoni: AG, GL, SH, SO, VD, ZH; organizzazioni: ASA, asut, curafutura, IGEM, privatim, santésuisse, Sunrise UPC, SWICO, swissICT, UTP. FFS, H+, la Posta, Migros, Ringier, suva, thurbo, UTP et Walderwyss chiedono almeno l'eliminazione della seconda frase.

[203] Cantoni: AG, BE, GL, NW, SH, SO, SZ, VD; organizzazioni: ATPrD, Migros, Incaricato cantonale della protezione dei dati SZ, OW e NW., Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim, santésuisse, suva.

coinvolto nell'attuazione delle norme sulla protezione dei dati. SO aggiunge che la disposizione non tiene sufficientemente conto di questo requisito. Secondo alcuni partecipanti[204], sembra contrario all'approccio basato sui rischi della nLPD che il consulente per la protezione dei dati sia informato solo *a posteriori* della conclusione di un contratto di esternalizzazione o in occasione del trasferimento di una funzione. I compiti del consulente per la protezione dei dati comprendono tali transazioni. Il rapporto esplicativo menziona espressamente i maggiori rischi associati al trattamento dei mandati. Inoltre, la partecipazione all'attuazione delle norme sulla protezione dei dati è uno dei suoi compiti principali. Il consulente per la protezione dei dati va informato in tempo utile, come previsto per i progetti degli organi federali per il trattamento automatizzato dei dati personali (art. 31). Come minimo, la disposizione andrebbe rafforzata.

Alcuni partecipanti[205] sono dell'opinione che questa disposizione violi la libertà organizzativa interna all'impresa. Un'impresa deve assicurarsi che i contratti siano conformi alle norme sulla protezione dei dati. Chiedono che le imprese di trasporto siano escluse dal campo d'applicazione della disposizione.

Due partecipanti[206] sottolineano che gli organi federali, come le compagnie di assicurazione malattie, hanno innumerevoli contratti che includono il trattamento di dati. L'approccio basato sui rischi richiede che, attraverso il registro delle attività di trattamento, il consulente per la protezione dei dati conosca i trattamenti particolarmente rischiosi. Un obbligo di informazione supplementare con un grado di assolutezza così elevato non è necessario, soprattutto in quanto non crea alcun valore aggiunto per le persone interessate.

Il DFS sottolinea che l'attività di prevenzione dei consulenti per la protezione dei dati è di grande importanza. Questo aspetto andrebbe preso in considerazione per la stesura di questo articolo, così da evitare il più possibile ulteriori problemi. L'idea sarebbe quella di stabilire una consulenza preventiva del consulente per la protezione dei dati, il che implica anche che egli faccia parte degli organi corrispondenti.

HDC ritiene che l'obbligo di informare il consulente per la protezione dei dati abbia dei vantaggi. Tuttavia, fatica a capirne il legame con la nLPD e le conseguenze della sua violazione. Si chiede se una delle conseguenze sarebbe quella di rendere il trattamento illegale e permettere all'interessato di far valere dei diritti su questa base (art. 41 nLPD). Alcuni partecipanti[207] sottolineano che l'articolo 29 nLPD prevede già un obbligo di informare formulato in modo più generale che copre anche i trattamenti su mandato, purché siano di rilievo.

L'ASIP chiede di specificare che «non s'intendono gli organi federali in qualità di responsabili ai sensi dell'articolo 2 capoverso 1 lettera b in combinato disposto con l'articolo 5 lettera i nLPD».

swissICT non comprende perché nell'ordinanza vengano fissati requisiti particolari, dato che l'articolo 24 LPD disciplina la notifica delle violazioni della sicurezza dei dati. I processi interni andrebbero disciplinati dall'organo federale stesso. Inoltre, l'articolo 29 capoverso 1 nDPA prevede già un obbligo d'informazione da parte dell'organo federale nei confronti del consulente per la protezione dei dati. AswissICT uspica un chiarimento del termine «problemi».

[204] Cantoni: AG, BE, GL, NW, SH, SZ, UR, VD, ZH; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[205] Organizzazioni: FFS, la Posta, thurbo, UTP.

[206] Organizzazioni: ASA, curafutura.

[207] Organizzazioni: asut, BNS, Sunrise UPC, suva, SWICO.

3.2.8 Art. 8 AP-OLPD: Valutazione dell'adeguatezza

VS accoglie con favore l'elaborazione di un elenco di Stati, settori e territori con un livello di protezione adeguato (allegato).

Alcuni partecipanti[208] chiedono il rispetto del principio di trasparenza, in particolare per quanto riguarda i capoversi 3-5. Questo principio dovrebbe trapelare non solo nei risultati, ma anche nel processo decisionale. Alcuni partecipanti[209] chiedono che la formulazione della disposizione chiarisca che è indirizzata in generale al Consiglio federale. Diversi partecipanti[210] ritengono che la procedura di valutazione andrebbe disciplinata, in particolare la procedura per ottenere la valutazione dell'adeguatezza, se è soggetta a ricorso, nonché i casi di esclusione. Andrebbero aggiunti i rimedi giuridici.

Il PPS teme che il trasferimento della valutazione dell'adeguatezza al Consiglio federale (art. 16 nLPD) porti a decisioni di natura politica e non basate su una perizia effettiva. Propone quindi che l'IFPDT continui ad effettuare la valutazione. Alcuni partecipanti[211] chiedono di aggiungere nella disposizione che il livello ritenuto adeguato è quello specificato nella nLPD.

Secondo GE, un elenco non esaustivo di Stati la cui legislazione fornisce un adeguato livello di protezione non è soddisfacente. Andrebbe preferito il mantenimento del sistema attuale ossia un elenco esaustivo. Questa soluzione faciliterebbe l'applicazione della legge - soprattutto da parte di privati e imprese private - e gli scambi con l'estero.

Alcuni partecipanti[212] lamentano la mancanza di informazioni nel rapporto esplicativo, in particolare per quanto riguarda i destinatari della disposizione e coloro che sono tenuti ad agire. Inoltre, poiché l'articolo non può ovviamente riguardare il titolare privato, ciò andrebbe precisato esplicitamente nel testo dell'ordinanza.

Classtime ritiene che la valutazione dell'adeguatezza andrebbe considerata nel contesto dell'uso di fornitori di servizi terzi stranieri. A titolo illustrativo, l'uso di prodotti Microsoft è diffuso, anche se Microsoft fa largo uso di fornitori di servizi terzi negli Stati Uniti (archivi di file e cloud storage). I divieti legali non sono affatto rispettati da queste multinazionali. Pertanto, i piccoli fornitori svizzeri che utilizzano fornitori di servizi terzi come responsabili, soprattutto negli Stati Uniti, non dovrebbero essere svantaggiati. Il trasferimento di dati personali per il trattamento da parte di fornitori di servizi terzi va reso molto meno rigido, così che sia *di fatto* applicabile e valutato in base alla sensibilità dei dati. Va inoltre osservato che gli organi pubblici usano questi prodotti.

Cpv. 1

HDC riconosce che un approccio basato su categorie (uno Stato, un territorio, un settore specifico) può rivelarsi opportuno. Ciò nonostante, questa classificazione deve avere una base legale. In sua assenza, si tratta di un procedimento *ultra legem*. Ad esempio, l'espressione «uno o più settori» non è definita. Ne consegue un rischio di interpretazione e di applicazione.

[208] Partiti: PPS, PVS.

[209] Partiti: Alleanza del Centro, organizzazioni: AFPS, ASB, Associazione di commercio, ASPS, asut, CURAVIVA Suisse, DigiGes, digitalswitzerland, economiesuisse, EXPERTsuisse, HÄRTING, HKBB, INSOS, IS, la Posta, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, senesuisse, SPITEX suisse, SPA, Fondazione per la protezione dei consumatori, Sunrise UPC, SWICO, SwissHoldings, usam.

[210] Organizzazioni: FRC, HDC, swissprivacy.law.

[211] Organizzazioni: HDC, FRC.

[212] Organizzazioni: Creditreform, vsi.

L'articolo 16 capoverso 3 nLPD lascia al Consiglio federale la possibilità introdurre garanzie da comunicare previamente all'IFPDT. Non si tratta di una valutazione dell'adeguatezza.

GL accoglie con favore l'aggiunta di una distinzione tra «Stato», «territorio» o «uno o più settori di uno Stato». Essa permette al Consiglio federale di tenere conto delle particolarità legali e/o locali nella sua valutazione dell'adeguatezza. FRC sottolinea che la possibilità di concedere un'autorizzazione quando un determinato settore di uno Stato fornisce un livello di protezione sufficiente deve essere subordinata al fatto che tale settore non sia soggetto alle leggi o a determinate leggi dello Stato in cui si trova. Allo stesso modo, solo i territori con autonomia legale dal punto di vista della protezione dei dati dovrebbero essere ammissibili. I criteri dovrebbero figurare nell'ordinanza. Secondo swissprivacy.law, l'articolo 8 differisce dall'articolo 16 nLPD per l'aggiunta di un territorio o di uno o più settori di uno Stato. Questa precisazione non corrisponde alla volontà del legislatore e va abolita.

Secondo diversi partecipanti[213], al capoverso va aggiunta una seconda frase, in particolare dopo l'elenco dei criteri (lett. a-e). La formula proposta è la seguente: «I responsabili possono basarsi sulla decisione del Consiglio federale in merito all'adeguatezza della protezione dei dati conformemente alla prima frase e non devono procedere a ulteriori chiarimenti».

UBCS ricorda che l'elenco stilato dal Consiglio federale (art. 16 cpv. 1 nLPD) è vincolante per tutti gli attori dell'adeguatezza. L'ulteriore esame caso per caso e la valutazione che ne consegue non sono né fattibili né appropriati.

Cpv 1 lett. b

GL accoglie con favore l'introduzione del criterio generale del «rispetto dei diritti dell'uomo».

Alcuni partecipanti[214] sottolineano che il rispetto dei diritti dell'uomo non è un criterio rilevante, in particolare a causa della sua mancanza di chiarezza. Tale criterio non ha ragion d'essere quando si tratta di determinare se uno Stato (o un territorio o un settore specifico) o un organismo internazionale fornisce un'adeguata protezione dei dati. La protezione dei diritti dell'uomo è senza dubbio un aspetto importante di cui tenere sempre conto: per esempio in occasione della valutazione del rispetto dei principi di protezione della personalità, per quanto riguarda i diritti dell'uomo a essa connessi. Il concetto di diritti dell'uomo si riferisce innegabilmente ai diritti fondamentali sanciti dalla Costituzione federale[215]. L'adeguatezza non dipende quindi dal fatto che uno Stato permetta la dissimulazione del volto nello spazio pubblico o non garantisca la libertà delle arti o il diritto all'istruzione a titolo gratuito.

Cpv. 1 lett: c

Secondo swissICT, l'inclusione della giurisprudenza è troppo restrittiva, inadatta alla pratica e mina la certezza del diritto. Questo imporrebbe di rivedere costantemente la valutazione ogni qualvolta venga emessa una nuova decisione sulla protezione dei dati. Propone di sostituire il testo come segue: «la legislazione in vigore in materia di protezione dei dati, la sua attuazione e la giurisprudenza pertinente».

Cpv. 1 lett. d

[213] Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, SDV, Scienceindustries suisse.

[214] Organizzazioni: FRC, HDC, swissprivacy.law, UPSC.

[215] Cost. fed., RS 101, articolo 7 segg.

FRC chiede di precisare che la garanzia di un processo equo è un criterio importante al fine di garantire una difesa equa alla persona i cui dati potrebbero essere utilizzati all'estero.

Cpv. 1 lett. e

Secondo swissICT, la lettera andrebbe eliminata. Come minimo, la formulazione dovrebbe ispirarsi ai criteri di valutazione della Commissione europea.

Cpv. 1 lett. f

Swimag vorrebbe aggiungere una lettera f a questo capoverso. Infatti, la persona o le persone i cui dati personali sono comunicati all'estero non devono essere private dei loro diritti. Non devono subire alcuno svantaggio in relazione alla non comunicazione, in particolare tra il diritto svizzero e il diritto straniero. Un esame attento e preventivo della legislazione applicabile è indispensabile. Determinare se uno Stato, un territorio, uno o più specifici settori di uno Stato o organismo internazionale garantisca un'adeguata protezione dei dati è di scarsa utilità senza i criteri aggiunti presenti in questo esame di diritto comparato.

Cpv. 1 lett. g

Swimag chiede inoltre di aggiungere che in tutti i casi di comunicazione di dati personali all'estero, è necessario il consenso scritto dell'interessato.

Cpv. 3

Alcuni partecipanti[216] ricordano che l'IFPDT informava regolarmente sugli sviluppi e gli adattamenti in corso tramite il proprio sito web. Il Consiglio federale dovrebbe rendere le sue decisioni accessibili al pubblico in modo trasparente. Si propone di completare il capoverso come segue: «Le decisioni, le modifiche e gli adattamenti vanno motivati e messi a disposizione del pubblico senza indugio e in modo completo».

Alcuni partecipanti[217] ritengono che gli intervalli tra le valutazioni vadano indicati in modo più preciso. Andrebbe aggiunto che «sono periodici, ma hanno luogo almeno una volta l'anno».

SPA propone di aggiungere al testo che l'obbligo di rivalutazione spetta al Consiglio federale.

Cpv. 4

Come l'articolo 16 capoverso 2 nLPD, l'articolo 8 capoverso 4 si riferisce al concetto di decisione. Secondo il TAF, occorre chiarire se si tratti di una decisione ai sensi dell'articolo 5 della legge federale sulla procedura amministrativa[218].

L'ASDPO vorrebbe che la procedura fosse chiarita, specificando in particolare se è possibile fare ricorso. Affermare che la nuova decisione non ha alcun effetto sui dati già comunicati all'estero è sbagliato. I dati già comunicati nell'ambito di una regola di adeguatezza sono trattati in uno Stato che (eventualmente) non offre un livello di protezione adeguato, il che può incidere

[216] Organizzazione: DigiGes ; partito: PVS. Allo stesso modo: Fondazione per la protezione dei consumatori

[217] Organizzazioni: ASDPO, ASPS, CURAVIVA suisse, INSOS, IS, senesuisse, SPITEX suisse.

[218] PA, RS 172.021.

sui diritti della personalità degli interessati. Come minimo, si chiede di cancellare la seconda frase.

SwissICT chiede cosa si intenda per «comunicazioni di dati già avvenute» e se questo capoverso sia applicabile se è garantita una protezione dei dati adeguata. per quanto riguarda i titolari del trattamento questa disposizione avrebbe dovuto essere inclusa nella legge. Swimag ritiene che la nuova decisione non abbia alcun impatto sulle comunicazioni già effettuate. È applicabile, per quanto possibile, alle comunicazioni già avvenute. Bisognerebbe evitare, compensare o rimediare ai danni a alle violazioni passati e futuri.

Cpv. 5

Il PVS chiarisce che l'IFPDT non deve essere solo consultato, ma le sue opinioni vanno anche materialmente prese in considerazione nella valutazione. Bisognerebbe adattare il capoverso in tal senso.

La FER ritiene che l'uso di un elenco «positiva» crei incertezza giuridica. Infatti, uno Stato che non figura nell'elenco può semplicemente non essere ancora stato oggetto di un esame del Consiglio federale. La pratica attuale va mantenuta: l'IFPDT pubblica un documento in cui accanto ad ogni Stato viene indicato se questo soddisfa un livello adeguato di protezione dei dati personali.

Cpv. 6

Alcuni partecipanti[219] propongono la seguente formulazione: «Il Consiglio federale consulta l'IFPDT prima di ogni decisione sull'adeguatezza della protezione dei dati». Affinché la decisione del Consiglio federale non sia politica, l'IFPDT va effettivamente consultato[220] o gli va addirittura concesso un diritto di veto[221]. Alcuni partecipanti[222] notano che l'IFPDT dovrebbe essere formalmente consultato. Le valutazioni delle organizzazioni internazionali o delle autorità straniere possono essere (materialmente) prese in considerazione. Si chiede di formulare esplicitamente, almeno nel rapporto esplicativo, che anche i pareri dell'IFPDT vanno concretamente presi in considerazione.

Cpv. 7

Per motivi di chiarezza, una minoranza tra i partecipanti[223] propone l'aggiunta di un capoverso 7 dal seguente tenore: «Se i dati personali sono comunicati all'estero in uno Stato o territorio che non dispone di una protezione dei dati adeguata, possono essere necessari provvedimenti aggiuntivi oltre alle garanzie previste dall'articolo 16 capoverso 2 lettere b e c LPD per assicurare un'adeguata protezione dei dati. Il Consiglio federale determina se siano necessari provvedimenti supplementari. Gli Stati e i territori interessati sono elencati nell'allegato 1a. La decisione del Consiglio federale sulla necessità di provvedimenti supplementari è vincolante».

[219] Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, SDV, Scienceindustries suisse, SPA, Fondazione per la protezione dei consumatori.

[220] Organizzazioni: DigiGes, Fondazione per la protezione dei consumatori.

[221] Organizzazione: Fondazione per la protezione dei consumatori.

[222] Cantoni: AG, BE, GL, NW, SH, SZ, VD, ZH; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

[223] Organizzazioni: ASB, digitalswitzerland, economiesuisse, HKBB, la Posta, le banche domestiche, Raiffeisen, SDV, Scienceindustries suisse.

3.2.9 Art. 9 AP-OLPD: Clausole di protezione dei dati e garanzie specifiche

Alcuni partecipanti[224] sostengono l'intenzione del Consiglio federale di introdurre determinati requisiti minimi e garanzie specifiche; tanto più che le clausole o garanzie (art. 16 cpv. 2 lett. b, nLPD) sono rese note solo all'IFPDT.

Tuttavia, sono critici in merito alle esigenze introdotte da questa disposizione. Il grado di dettaglio è considerato inutile[225].

HÄRTING si rammarica che i requisiti di questo articolo non si concentrino maggiormente sui ruoli di esportatore (titolare del trattamento) e importatore (destinatario).

Cpv. 1

La FSA ritiene che l'elenco sia illustrativo. In caso contrario, andrebbe chiarito che va fatta una distinzione tra i contratti in cui il destinatario è un titolare del trattamento e quelli in cui opera in qualità di responsabile.

Alcuni partecipanti[226] sono dell'opinione che, sebbene coerenti con l'obiettivo della protezione dei dati, questi requisiti implicano costi elevati per le imprese coinvolte. Pertanto, andrebbero ridotti al minimo, o almeno le lettere b, c, g, h e i andrebbero eliminate.

Alcuni partecipanti[227] ritengono che l'elenco dei requisiti di un «Data Transfer Agreement» sia inadatto e vada cancellato. A questo proposito, bisogna precisare che l'IFPDT deve controllarli in ogni caso. Tuttavia, questo elenco non distingue tra il tipo di trasferimento o tra il ruolo di esportatore e di importatore. Questi ultimi sono però determinanti per il contenuto del contratto, come mostrano le clausole contrattuali standard della Commissione europea (EU SCC). Va sottolineato che tali clausole sono ormai riconosciute dall'IFPDT. Quindi, non ha senso imporre obblighi ai responsabili tramite contratto, qualora tali obblighi non si basino sulla nLPD. Il RGPD fornisce una protezione adeguata. Questa protezione vale anche per i dati comunicati da titolari svizzeri del trattamento. Come minimo è opportuno modificare l'elenco dei requisiti in modo da coprire diverse costellazioni (titolare del trattamento, responsabile) o sostituire «almeno» con «a seconda delle circostanze». Infine, e nella misura in cui gli interessati vanno informati, mancano regole sulla notifica delle violazioni della sicurezza dei dati. Anche altri partecipanti[228] si interrogano sulla questione della base legale. Inoltre specificano che i criteri non dovrebbero essere assoggettati a tutti i possibili sistemi giuridici cumulativamente, il che sarebbe difficile per il titolare del trattamento.

L'ASDPO nota che manca un punto sul diritto di controllo dell'esportatore di dati nei confronti dell'importatore. Propone quindi di aggiungere una lettera m sul diritto di audit e una lettera n sulla segnalazione delle violazioni della sicurezza dei dati.

La Posta è del parere che le lettere d, e, f e j siano da eliminare.

---

[224] Partito: PS; organizzazione: USS.

[225] Organizzazioni: CURAVIVA suisse, EXPERTsuisse, SPITEX suisse, usam.

[226] Organizzazioni: ASPS, CURAVIVA suisse, digitalswitzerland, economiesuisse, EXPERTsuisse, HKBB, INSOS, IS, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, senesuisse, SPITEX suisse.

[227] Organizzazioni: ASB, asut, FFS, digitalswitzerland, economiesuisse, DFS, H+, HKBB, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, Sunrise UPC, suva, SWICO, thurbo, UTP, VUD, Walderwyss.

[228] Organizzazioni: Creditreform, Datenschutzguide.ch, vsi.

Alcuni partecipanti[229] notano la mancanza di distinzione tra i ruoli di esportatore e importatore. Si chiedono se non sarebbe più pratico sostituire in toto il testo dell'articolo 9 e conformarlo all'articolo 28 paragrafo 4 RGPD, dato che nella pratica è già vincolante.

Secondo Bär & Karrer, le lettere a-k definiscono il contenuto minimo delle clausole di protezione dei dati. Il RGPD non comprende tali elenchi (art. 43 par. 3 RGPD). Disciplina soltanto il contenuto minimo delle regole interne vincolanti sulla protezione dei dati. Secondo Walderwyss, a mancare sono gli accordi su come esaminare o prendere in considerazione le legislazioni locali e la procedura da seguire in caso di accesso da parte delle autorità.

Cpv. 1 lett. a

Alcuni partecipanti[230] sottolineano la mancanza del principio di trasparenza che quindi andrebbe aggiunto.

Cpv. 1 lett. d ed e

Secondo alcuni partecipanti[231], menzionare i nomi degli Stati o delle organizzazioni internazionali a cui vengono comunicati i dati personali non ha una base legale, in caso di ulteriore trasmissione. Anche la questione dell'ulteriore trasmissione va chiarita. Tuttavia, è sufficiente designare il destinatario. Anche le clausole contrattuali standard della Commissione europea si limitano a questo. SwissICT ritiene che manchi una base legale per esigere che vengano menzionati gli Stati o le organizzazioni a cui vengono trasmessi i dati. Di conseguenza, chiede l'eliminazione di queste lettere.

Cpv. 1 lett. f

Diversi partecipanti[232] non capiscono il senso della lettera, che è ridondante poiché già coperta dal principio della proporzionalità. La Posta ritiene, inoltre, che manchi una base legale.

Cpv. 1 lett. g

Alcuni partecipanti[233] ritengono che l'espressione «autorizzati a trattare i dati» sia inadatta, se non addirittura superflua. Secondo il loro parere, sono rilevanti solo i «destinatari», cioè le parti che stipulano il contratto. SwissICT propone lo stralcio della lettera.

Cpv. 1 lett. h

Diversi partecipanti[234] sono del parere che le misure per garantire la sicurezza dei dati personali sono già incluse nella clausola di protezione dei dati o nelle garanzie specifiche stesse, conformemente all'articolo 9 capoverso 2. Quindi, l'obbligo rinnovato per il titolare di adot-

[229] Organizzazioni: Bär & Karrer, swissICT.

[230] Organizzazioni: ASDPO, FFS, digitalswitzerland, economiesuisse, H+, HKBB, la Posta, le banche domestiche, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, thurbo, UTP, VUD, Walderwyss.

[231] Organizzazioni: FFS, digitalswitzerland, economiesuisse, H+, HKBB, la Posta, le banche domestiche, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, thurbo, UTP, VUD, Walderwyss.

[232] Organizzazioni: FFS, digitalswitzerland, economiesuisse, H+, HKBB, la Posta, le banche domestiche, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[233] Organizzazioni: FFS, digitalswitzerland, economiesuisse, H+, HKBB, la Posta, le banche domestiche, Raiffeisen, Ringier, Scienceindustries suisse, SDV, SPA, suva, swissICT, thurbo, UTP, VUD, Walderwyss.

[234] Organizzazioni: Digitalswitzerland, economiesuisse, HKBB, HotellerieSuisse, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, usam.

tare misure adeguate a garanzia del rispetto delle clausole sulla protezione dei dati è ridondante. Il rispetto di tali clausole andrebbe invece garantito obbligando per iscritto il destinatario a rispettare o osservare le clausole di protezione dei dati. Questi partecipanti non vedono la necessità di questa lettera e la trovano sproporzionata. La disposizione va abrogata.

ASDPO propone la seguente formulazione: «i provvedimenti tecnici e organizzativi».

Cpv. 1 lett. j

Due partecipanti[235] ritengono che non sia responsabilità del responsabile del trattamento informare gli interessati. Quindi, chiede di introdurre nelle clausole di protezione un obbligo per i destinatari di informare gli interessati. Al contrario, BE è del parere che questa lettera vada cancellata. Secondo gli articoli 19-23 nLPD, l'obbligo d'informazione riguarda solo le autorità responsabili. Un'estensione dell'obbligo al destinatario dei dati pare poco ragionevole e di difficile realizzazione.

Alcuni partecipanti[236] ritengono che il nuovo obbligo andrebbe incluso in una base legale formale. Suisa ritiene che questa lettera contraddica l'articolo 19 capoverso 4 e l'articolo 25 capoverso 1 nLPD. Queste due disposizioni definiscono in modo esaustivo la portata dell'obbligo d'informare. Inoltre, questa lettera è spesso inapplicabile da un punto di vista puramente pratico, poiché il destinatario dei dati all'estero non può identificare, in base ai dati ricevuti, le persone interessate e i loro indirizzi per poterle informare. Si chiede l'eliminazione di questa lettera.

Santésuisse considera questa lettera imprecisa e s'interroga sulle ragioni che obbligano il destinatario a informare le persone interessate. Questo dovrebbe restare di competenza del titolare del trattamento, poiché non si tratta di un'esternalizzazione ai sensi dell'articolo 9 nLPD. Inoltre, va notato che non è spiegato cosa si intenda per «informare del trattamento». SwissICT propone l'eliminazione della lettera. A questo proposito si riferisce all'osservazione sull'articolo 9 capoverso 1 in merito alla mancanza di distinzione secondo i ruoli delle parti.

HÄRTING sottolinea che, se si tratta di un «trasferimento a termine», bisognerebbe fare riferimento alla lettera i. Si può lasciare aperta la questione se il dovere di informare debba essere imposto all'esportatore o all'importatore.

Cpv. 1 lett. k

Suisa ritiene che il nuovo obbligo andrebbe formalmente incluso in una base legale. Ritiene che il capoverso 1 contraddica l'articolo 19 capoverso 4 e l'articolo 25 capoverso 1 nLPD. Queste ultime due disposizioni legali definiscono in modo esaustivo la portata dell'obbligo d'informare. Inoltre, questa disposizione porterebbe all'applicazione extraterritoriale del diritto svizzero, cosa contraria al diritto internazionale e quindi impossibile da attuare. Chiede la cancellazione di questa lettera.

SwissICT chiede di abrogare questa lettera. Nel caso della comunicazione nel contesto del trattamento dell'ordine, ciò non è legittimo. Si fa riferimento all'osservazione generale dell'articolo 9 capoverso 1. Propone anche di aggiungere un riferimento tra parentesi alla disposizione della LPD in cui questo diritto della persona interessata è disciplinato.

[235] Organizzazioni: ASA, curafutura.

[236] Organizzazioni: Suisa, Walderwyss.

Secondo HÄRTING, la nLPD riconosce solo il diritto dell'interessato di opporsi alla comunicazione di dati personali da parte dell'organo federale responsabile (art. 37 nLPD). L'articolo 9 capoverso 1 lettera k probabilmente non si riferisce a questo diritto. Il rapporto esplicativo si riferisce al «diritto di opporsi al trattamento dei dati personali». Non è chiaro a quale diritto degli interessati contenuto nella nLPD si faccia riferimento; probabilmente al diritto dell'interessato di revocare il suo consenso in qualsiasi momento e quindi la lettera k dovrebbe essere adattata di conseguenza.

L'ASDPO propone di aggiungere il diritto di consegnare i dati (art. 28 e 29 nLPD).

Swimag propone l'aggiunta di un numero 5 con la seguente formulazione: «non acconsentire al trattamento dei dati».

Cpv. 2

CFC vorrebbe degli esempi di «misure appropriate». Questo permetterebbe una migliore comprensione della situazione da parte del titolare del trattamento nonché della persona interessata.

Secondo alcuni partecipanti[237], il verbo «garantire» è un po' eccessivo. Alcuni spiegano che il verbo implica una garanzia di rispetto delle clausole o una responsabilità causale, per la quale non esiste alcuna base legale. Quindi tale obbligo non può essere ragionevolmente richiesto. Propongono di scegliere la seguente formulazione: «controllare» o «controllare in modo adeguato». Inoltre, alcuni partecipanti[238] ritengono questo capoverso troppo vago. Si domandano quali potrebbero essere queste misure, soprattutto perché il RGPD non prevede un tale disciplinamento. Questo capoverso va abolito.

Diversi partecipanti[239] sottolineano che le clausole di protezione dovrebbero contenere l'obbligo per il destinatario di informare gli interessati. Non spetta al responsabile del trattamento informare gli interessati. Questa è una responsabilità del titolare del trattamento.

Cpv. 3

Alcuni partecipanti[240] ritengono che secondo l'articolo 16 capoverso 2 lettere b e c nLPD, le clausole di protezione dei dati e le garanzie specifiche vadano comunicate preliminarmente all'IFPDT. Chiedono che la frase introduttiva dell'articolo 9 capoverso 3 sia rivista o che sia adattato addirittura l'intero capoverso. Il capoverso suggerisce infatti che potrebbe presentarsi una situazione in cui la non comunicazione porterebbe a una comunicazione all'estero conforme al diritto. SH insiste che il capoverso non dovrebbe indebolire l'articolo 16 capoverso 2 lettere b e c nLPD. Secondo VD, bisogna sottolineare che nel contesto del RGPD e dei trattamenti e trasferimenti tra persone giuridiche della stessa entità o appartenenti allo stesso gruppo, queste ultime vadano considerate come terzi. Pertanto, vanno richiesti un contratto di esternalizzazione e delle clausole di protezione. L'UPSC ritiene che il fatto che, prima della comunicazione all'estero, i dati siano semplicemente trasmessi all'IFDPT, senza che quest'ultimo debba approvare le garanzie specifiche, crei un rischio significativo che la valutazione dei rischi da parte dei titolari del trattamento e dei responsabili sia diversa, sia nel settore privato

[237] Organizzazioni: ASP, Associazione di commercio, Creditreform, curafutura, economiesuisse, EPS, FSA, VSP, IGEM, HotellerieSuisse, SPA, suva, Swissstaffing, usam, vsi.

[238] Organizzazioni: asut, Sunrise UPC, SWICO, swissICT.

[239] Organizzazioni: digitalswitzerland, economiesuisse, HKBB, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV,.

[240] Cantoni: AG, BE, GL, NW, SZ, VD; organizzazioni: ATPrD, Incaricato cantonale della protezione dei dati SZ, OW e NW, Incaricato cantonale della protezione dei dati e della trasparenza NE/JU, privatim.

che in quello pubblico. Si chiede che questa semplice informazione sia sostituita da un obbligo di approvazione dell'IFPDT.

3.2.10 Articolo 10 AP-OLPD: Clausole tipo di protezione dei dati

Alcuni partecipanti[241] accolgono con favore questa disposizione, e in particolare il fatto che l'IFPDT pubblica un elenco di clausole tipo di protezione dei dati. Inoltre, CFC chiede esempi di criteri per valutare l'appropriatezza delle misure.

In generale, si chiede la cancellazione della disposizione o il suo adattamento.[242] In riferimento all'introduzione di clausole tipo di protezione dei dati, la disposizione è considerata eccessiva[243] e persino superflua[244]. È considerata troppo vaga, poiché non precisa quali potrebbero essere queste misure[245]. Sono necessarie precisazioni. Il rapporto esplicativo dovrebbe menzionare che i destinatari non sono obbligati a rispettare la legislazione svizzera sulla protezione dei dati (art. 6 cpv. 2 nLPD)[246].

Il TAF mette in discussione la «forma giuridica» delle clausole tipo di protezione dei dati pubblicate dall'IFPDT. A suo avviso, non può trattarsi di una decisione impugnabile ai sensi dell'articolo 5 capoverso 1 PA, in particolare quando l'IFPDT le stabilisce d'ufficio, in assenza di una richiesta esplicita da parte dell'amministrato. Osserva che la pubblicazione di clausole tipo non crea, modifica o cancella i diritti e gli obblighi di un privato e non è destinata ad essere applicata a un caso specifico. Dal suo punto di vista, si tratta di una raccomandazione generale e astratta. La verifica della conformità della comunicazione con le norme sulla protezione dei dati andrebbe effettuata *ex post*, nel quadro di un'inchiesta da parte dell'IFPDT, che porterebbe, soltanto in quel caso, a una decisione impugnabile (art. 52 nLPD).

Cpv. 1

Come per le disposizioni precedenti, si richiede che, invece del dovere di «garantirne» il rispetto, il titolare del trattamento «provveda affinché» il destinatario rispetti le clausole tipo di protezione dei datiin particolare attraverso un audit[247]. Santésuisse ritiene che quest'obbligo sia impossibile da attuare in riferimento alle disposizioni penali. Alcuni partecipanti[248] spiegano che questo capoverso comporta una responsabilità causale e sarebbe impossibile da rispettare. Come minimo, il titolare del trattamento deve adottare provvedimenti adeguati per contribuire a garantire che il destinatario rispetti le clausole.

La Suva afferma che le misure sono appropriate se corrispondono allo stato della tecnica e alle circostanze specifiche. Le attuali clausole tipo, ampiamente utilizzate nella pratica, richiedono comunque corrispondenti obblighi di diligenza da parte dell'esportatore.

---

[241] Organizzazioni: ASPS, CURAVIVA, INSOS, IS, senesuisse, SPITEXsuisse.

[242] Organizzazione: ASB, ASP, ASSL, Associazione di commercio, asut, auto suisse, CFC, FFS, Creditreform, EPS, FER, FSA, VSP, H+, HÄRTING, HotellerieSuisse, IGEM, la Posta, le banche domestiche, Migros, Raiffeisen, Ringier, santésuisse, SPA, Sunrise UPC, suva, SWICO, Swiss Insights, swissICT, TAF, thurbo, UPSA, UTP, vsi, VUD, Walderwyss.

[243] Organizzazioni: HotellerieSuisse, vsi.

[244] Organizzazioni: asut, HotellerieSuisse, Sunrise UPC, SWICO, swissICT, Walderwyss.

[245] Organizzazioni: asut, digitalswitzerland, economiesuisse, HKBB, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, Sunrise UPC, SWICO, swissICT.

[246] Organizzazioni: auto suisse, digitalswitzerland, economiesuisse, HKBB, le banche domestiche, Raiffeisen, Scienceindustries suisse, SDV, Swiss Insights.

[247] Organizzazioni: ASB, ASP, Associazione di commercio, auto suisse, EPS, FSA, VSP, HÄRTING, HotellerieSuisse, IGEM, la Posta, le banche domestiche, Raiffeisen, SPA, swissICT, Swiss Insights, suva, Swissstaffing, usam, vsi, Walderwyss.

[248] Organizzazioni: ASB, la Posta, le banche domestiche, suva, swissICT.

Auto suisse sottolinea che l'adeguatezza delle misure richieste dipende dalle circostanze del caso specifico e che i requisiti sono più elevati, in particolare quando sono coinvolti dati personali sensibili.

Capoverso 2

Alcuni partecipanti[249] sostengono la pubblicazione da parte dell'IFPDT di un elenco di clausole tipo di protezione dei dati.

3.2.11 Art. 11 AP-OLPD: Norme interne dell'impresa vincolanti sulla protezione dei dati

Cpv. 1

Si desidera un chiarimento su quando un'impresa appartiene allo stesso gruppo[250]. ASDPO chiede se le imprese di un gruppo debbano essere possedute per più del 50 % dagli stessi proprietari di quote e come vadano valutate le succursali. HÄRTING Rechtsanwälte descrive che, di norma, si parla di imprese congiunte se una società unisce una o più società sotto una gestione uniforme attraverso una maggioranza di capitale o di voti.

Classtime nota che le Binding Corporate Rules (BCR)[251] dovrebbero essere applicate anche a tutti i fornitori di servizi che hanno una relazione contrattuale diretta[252].

Cpv. 2

EXPERTsuisse nota che la portata dell'articolo 11 AP-OLPD è meno ampia rispetto all'articolo 47 RGPD. Tuttavia, le precedenti BCR sarebbero sempre state formulate in modo da essere conformi all'UE. FER nota invece che i requisiti vanno oltre l'articolo 16 capoverso 2 lettera e nLPD e che la lettera a imita il RGPD. Questo non è necessario e sarebbe sufficiente lasciare la lettera b.

Inoltre, FER osserva che l'articolo 6 capoverso 5 dell'attuale OLPD prevede che l'IFPDT esamina le garanzie e le regole sulla protezione dei dati che gli sono state comunicate e comunica il risultato del suo esame al detentore della collezione di dati entro un termine di 30 giorni, senza obbligarlo a condividere le informazioni richieste dall'articolo 11 capoverso 2 lettera a AP-OLPD. In questo senso, FER auspica che anche l'articolo 11 AP-OLPD contenga un termine per la comunicazione del risultato da parte dell'IFPDT. Il termine di 30 giorni dell'articolo 6 capoverso 5 dell'OLPD vigente andrebbe mantenuto.

3.2.12 Art. 12 AP-OLPD: Codici di condotta e certificazioni

Cpv. 2

Singoli partecipanti alla consultazione sono dell'opinione che, essendo per sua natura astratto e non formulato per imprese specifiche, il codice di condotta non possa contenere le informazioni di cui all'articolo 9 capoverso 1 AP-OLPD. Idealmente, quindi, i punti dell'articolo 9

[249] Organizzazioni: ASPS, CURAVIVA suisse, INSOS, IS, senesuisse, SPITEX suisse.

[250] Organizzazioni: ASDPO, HÄRTING.

[251] Le norme vincolanti d'impresa (Binding Corporate Rules - BCRs) sono direttive per la protezione dei dati seguite dalle imprese con sede nell'UE quando esse trasferiscono dati personali a Paesi al di fuori dell'UE all'interno di un gruppo di aziende o imprese. Tali regole devono includere tutti i principi generali di protezione dei dati e i diritti applicabili per assicurare garanzie adeguate per i trasferimenti di dati. Devono essere giuridicamente vincolanti e applicate da ogni socio interessato del gruppo di imprese.

[252] p. es. consulenti, freelance, sviluppatori, agenzie.

capoverso 1 AP-OLPD dovrebbero essere disciplinati solo secondo il loro significato e scopo.[253]

UPSC nota che i codici di condotta e le certificazioni devono essere approvati dall'IFPDT, anche se l'articolo 9 AP-OLPD, a cui si fa riferimento, prevede solo l'informazione e non l'approvazione da parte dell'IFPDT. Non essendo chiaro quando l'IFPDT debba solo essere informato e quando si applichi un obbligo di approvazione, si chiede un'armonizzazione. ASDPO desidera eliminare l'approvazione da parte dell'IFPDT.[254] USS e PS, d'altra parte, accolgono espressamente l'obbligo di approvazione. Classtime chiede delle «classi di sensibilità» nell'applicazione dell'articolo 12 AP-OLPD, al fine di garantire il principio di proporzionalità.

Infine, VUD vorrebbe che si parlasse di «disciplinamenti» o «punti» piuttosto che di «indicazioni».

Cpv. 3

Il Cantone di Soletta osserva che il carattere dell'«impegno esecutorio» va specificato poiché in alcuni Stati gli obblighi legali sarebbero applicabili in teoria, ma non nella pratica. È importante che l'esecuzione sia possibile senza sforzi sproporzionati.

Alcuni partecipanti alla consultazione osservano che non è chiaro se i requisiti derivati dall'articolo 12 capoversi 2 e 3 AP-OLPD non limitino irragionevolmente il campo di applicazione dei codici e delle certificazioni. Occorrerebbe piuttosto prestare attenzione all'effetto complessivo degli strumenti e, se necessario, farli approvare all'IFPDT. Pertanto, si dovrebbe prevedere una deroga all'applicazione dei capoversi 2 e 3 se l'IFPDT approva il codice di condotta o la certificazione.[255]

Rapporto esplicativo

Il Cantone di Soletta osserva che andrebbe chiarito dal rapporto esplicativo che i codici di condotta possono provenire solo dalle associazioni e non da singoli titolari.

3.2.13 Art. 13 AP-OLPD: Modalità degli obblighi di informare

Cpv. 1

La disposizione è espressamente accolta con favore da due partecipanti alla consultazione. È essenziale per il diritto all'autodeterminazione degli individui interessati, che possono così far valere i loro diritti.[256] In molti desiderano che il responsabile del trattamento dei dati sia cancellato dalla norma e in generale dall'AP-OLPD, poiché l'obbligo di fornire informazioni da parte sua è impraticabile e inutile.[257] Non esiste una base legale per i suoi obblighi. La nLPD non prevede la responsabilità del responsabile del trattamento dei dati.[258] Le autorità cantonali della protezione dei dati di Neuchâtel e del Giura osservano inoltre che la formulazione dell'articolo 13 capoverso1 AP-OLPD non è conforme alla gerarchia delle norme e appare molto estesa rispetto al testo della nLPD, tanto più che la distinzione tra il titolare e il responsabile è altrimenti osservata in tutta la nLPD. Anche se il capitolo 2 è intitolato «Obblighi del titolare e

[253] Organizzazioni: VUD, IGEM, suva.

[254] Allo stesso modo l'organizzazione: Classtime.

[255] Organizzazioni: Creditreform, usam, vsi.

[256] Organizzazioni: DigiGes, FRC.

[257] Cantoni: BE; partiti: Alleanza del centro; organizzazioni: UPSA, curafutura, EXPERTsuisse, ASSL, BNS, SSO, ASA.

[258] Cantoni: BE, LU, ZH; partiti: Alleanza del centro, PLR; organizzazioni: auto schweiz, curafutura, Coop, DFS, Datenschutzguide.ch, economiesuisse, HotellerieSuisse, HÄRTING Rechtsanwälte, IGEM, proFonds, santésuisse, FSA, ASB, SDV, BNS, SPA, SSO, UCS, ASA, SWICO, swissICT, swissstaffing, suva, Walderwyss, UBCS, VUD.

del responsabile del trattamento», è dubbio che il legislatore abbia voluto imporre al responsabile del trattamento gli stessi obblighi del titolare del trattamento. Il titolo risulta a priori dall'obbligo imposto ai responsabili del trattamento nell'articolo 24 capoverso 3 nLPD.

Inoltre, la responsabilità del responsabile del trattamento contraddice anche la logica della nLPD.[259] I responsabili del trattamento dei dati eseguono i loro compiti solo secondo le istruzioni ed esclusivamente secondo lo scopo specificato dai titolari del trattamento. Secondo l'articolo 19 e seguenti nLPD, l'obbligo d'informazione spetta solo alle autorità responsabili, ma non ai responsabileìi del trattamento. Questi ultimi devono solo rispettare gli obblighi contrattuali o le prescrizioni legali.[260] De facto, la relazione contrattuale concordata verrebbe così annullata o quantomeno gravemente compromessa. Il titolare perderebbe la sua funzione di principale e, in questo contesto, il suo dovere di sorvegliare il responsabile.[261] Anche se si potrebbe ricorrere a una delega contrattuale dell'adempimento degli obblighi, sarebbe fondamentalmente «contrario al sistema» ritenere entrambe le parti responsabili allo stesso tempo. Sarebbe tutt'al più possibile sostituire «e» con «o».[262]

Inoltre, secondo ABES, se il responsabile del trattamento è responsabile, persiste il rischio che l'informazione venga comunicata all'interessato più di una volta, portando a dichiarazioni contraddittorie. Inoltre, il responsabile spesso non possiede le informazioni desiderate o non è chiaro quali informazioni possano e debbano essere date a chi.[263] Inoltre, poiché secondo l'articolo 60 nLPD il mancato rispetto dell'obbligo è punibile, sono resi perseguibili anche il responsabile dei dati o le persone che agiscono per suo conto.[264]

In questo contesto, le autorità cantonali della protezione dei dati di Neuchâtel e del Giura lamentano che, mancando una regola di coordinamento, la norma è difficilmente applicabile nella pratica. Si pone la questione di chi sarebbe perseguito in caso di violazioni secondo l'articolo 60 nLPD. Il Cantone di Vaud ritiene che il coordinamento tra il titolare e il responsabile vada chiaramente disciplinato. Il Cantone di Svitto critica che la disposizione è formulata in modo poco chiaro e implica che il titolare e il responsabile del trattamento debbano informarsi a vicenda.[265] Anche SWICO nota che il capoverso 1 in combinazione con le spiegazioni è complessivamente impreciso. Ciò crea incertezza giuridica. Curafutura ritiene che, nell'interesse della certezza del diritto, andrebbe chiarito come adempiere il dovere di informare.[266]

Si osserva anche che l'obbligo del responsabile del trattamento, costuitirebbe uno swiss finish.[267] Secondo l'ASB, ciò renderebbe più difficile il traffico transfrontaliero dei dati personali in relazione all'UE. Questo sarebbe contrario a uno degli scopi principali della revisione.

Oltre alla questione degli obblighi del responsabile del trattamento, sono criticati anche altri punti. VUD osserva che l'articolo 19 nLPD richiede che la persona interessata sia informata. A questo scopo è sufficiente «rendere accessibile». La scelta del verbo «comunicare» non dovrebbe implicare alcun inasprimento. Pertanto, «mettere a disposizione» sarebbe un'espres-

[259] E, per inciso, anche la logica del GDPR. Organizzazioni: Econmiesuisse, la Posta, ASSOCIAZIONE DI COMMERCIO.swiss, UCS, Scienceindustries Switzerland, UBCS, FMH, Migros, SwissHoldings, FSA, Raiffeisen,

[260] Cantoni: BE, LU, ZH, partiti: Alleanza del centro, PLR, organizzazioni: ASDPO, curafutura, la Posta, economiesuisse, EXPERTsuisse, FMH, HANDELSVERBAND.swiss, Migros, proFonds, Raiffeisen, FSA, ASB, Scienceindustries Switzerland, UCS, ASA, SWICO, vsi, VUD.

[261] Organizzazioni: la Posta, ASB.

[262] Organizzazioni: Creditreform, ASSOCIAZIONE DI COMMERCIO.swiss, vsi.

[263] Anche l'organizzazione: economiesuisse.

[264] Organizzazioni: economiesuisse, SwissHoldings.

[265] Cantoni: SZ; organizzazione: UCS.

[266] Anche le organizzazioni: ProFonds, ASA.

[267] Partiti: PLR; organizzazioni: digitalswitzerland, economiesuisse, ASB, SwissHoldings, UBCS.

sione migliore. Questo esprimerebbe anche meglio il concetto secondo cui le persone interessate sono, in una certa misura, tenute a cooperare.[268] Inoltre, corrisponde alle intenzioni del RGPD.[269]

I Verdi, così come DigiGes, vorrebbero inserire «trasparente» nell'enumerazione relativa al modo di informare, poiché il termine figura nel RGPD.[270] Walderwyss trova l'enumerazione di «in forma precisa, comprensibile e facilmente accessibile» superflua in considerazione del requisito della trasparenza.

Un'altra questione importante è il «primo livello di comunicazione». In riferimento al rapporto esplicativo, si desidera che l'informazione non venga già fornita al primo livello di comunicazione. Alcuni partecipanti ritengono le spiegazioni a questo proposito nel rapporto esplicativo semplicemente sbagliate, poiché non sussiste alcuna base legale.[271] L'articolo 19 capoverso 1 nLPD sancisce che l'informazione deve essere «adeguata». Dal criterio di adeguatezza dell'articolo 19 capoverso 1 nLPD si evince che la comunicazione dipende dalle rispettive circostanze.[272] Tuttavia, le spiegazioni del rapporto esplicativo in merito all'articolo 13 capoverso 1 AP-OLPD implicano una regolamentazione significativamente più severa e quindi un inasprimento.[273]

VUD sostiene che l'«adeguatezza» dovrebbe anche tenere conto degli interessi e le aspettative di informazione delle persone interessate. Per esempio, non sono usuali riferimenti alla dichiarazione sulla protezione dei dati su biglietti da visita, carta intestata o nelle e-mail. Non dovrebbe nemmeno essere necessario riferirsi esplicitamente alla dichiarazione sulla protezione dei dati nelle situazioni quotidiane, ad esempio quando si prende un appuntamento allo sportello.[274] In questo senso, Bär & Karrer afferma che il disciplinamento è sproporzionato, impraticabile e inutilmente oneroso. Al contrario, le informazioni sul sito web dovrebbero essere sufficienti poiché in linea con la pratica attuale.[275] Secondo Raiffeisen, l'obbligo d'informazione potrebbe anche essere rispettato, per esempio, inserendolo nelle condizioni generali. Walderwyss osserva che l'obbligo di informare non richiede una notifica legale, ma piuttosto una dichiarazione di trattamento analoga a quella prevista dalla legge federale sull'informazione dei consumatori. Pertanto, è sufficiente rendere consultabili le informazioni pertinenti.

La Posta critica anche il fatto che il rapporto esplicativo sbaglia quando prevede l'adempimento dell'obbligo di informare per telefono. Per quanto riguarda le sanzioni penali, le problematiche probatorie che ne derivano sono irragionevoli.

Infine, si osserva che l'espressione «informazioni più importanti» non è chiara e va precisato quando il rapporto esplicativo afferma che «scegliere le modalità di comunicazione di modo che le informazioni più importanti siano sempre trasmesse al primo livello di comunicazione con la persona interessata».[276]

[268] Organizzazioni: economiesuisse, EXPERTsuisse, IGEM, SNB, SPA.

[269] Organizzazioni: SPA, suva, swissICT, Walderwyss.

[270] Partiti: GPS; organizzazione: DiGes.

[271] Organizzazioni: UPSA, auto schweiz, IGEM, USI, ASSL, suva, Swiss Insights, VUD.

[272] Organizzazioni: UPSA, economiesuisse, usam, ASSL, Swiss Insights, VUD.

[273] Organizzazioni: UPSA, GastroSuisse, HotellerieSuisse, ASB, usam (mutatis mutandis), ASSL, Swiss Insights.

[274] Anche le organizzazioni: UPSA, auto schweiz, economiesuisse, ASSL, Swiss Insights.

[275] Organizzazioni: ABES (per analogia), Bär & Karrer, la Posta, economiesuisse, HotellerieSuisse, IGEM, Migros, Raiffeisen, BNS, SPA, suva, ASA, SWICO, swissICT, VUD, Walderwyss.

[276] Organizzazioni: UPSA, auto schweiz, economiesuisse, HotellerieSuisse, ASB, ASSL, Swiss Insights.

Inoltre, nel capoverso 1, nonché in tutta l'ordinanza, si presta molta attenzione alla forma elettronica. Soprattutto in vista del futuro digitale, andrebbe disciplinato che le informazioni possono ora essere rese disponibili non solo su carta, ma anche elettronicamente.[277] ProFonds afferma che le spiegazioni del rapporto esplicativo non sono chiare per quanto riguarda la questione di come il titolare debba adempiere all'obbligo di informare nel settore non digitale;per esempio, se in caso di richiesta telefonica vadano lette diverse pagine di dichiarazione sulla protezione dei dati. Alcuni osservano che secondo il rapporto esplicativo è esplicitamente possibile anche la comunicazione in «forma elettronica», ad esempio tramite un sito web.[278] Il riferimento a un sito web o alle condizioni generali dovrebbe essere sufficiente al giorno d'oggi.[279] ProFonds nota che non è chiaro cosa intenda il rapporto esplicativo per «buona pratica», quando tutte le informazioni sono «disponibili a colpo d'occhio».

Alcuni partecipanti accolgono con favore la rinuncia a cambi di supporto. che andrebbe evitato e la norma va quindi mantenuta nella sua forma attuale.[280]

Capoverso 2

Il capoverso 2 è respinto dal mondo economico. È difficilmente comprensibile e non porta alcun valore aggiunto. Inoltre, è impraticabile.[281] VUD osserva innanzitutto che è discutibile fino a che punto il confronto di diversi documenti e in generale un certo grado di automazione costituiscano, come affermato nel rapporto esplicativo, un obiettivo della protezione dei dati.[282] La norma manca anche di una base legale.[283] La revisione della legge sulla protezione dei dati era stata discussa in dettaglio in Parlamento ed è il risultato di un compromesso. Pertanto, l'ordinanza non può introdurre requisiti aggiuntivi riguardanti l'obbligo di informare.[284] L'uso dei pittogrammi è facoltativo e in tal senso i pittogrammi andrebbero usati solo come supplemento e quindi per essi non andrebbe imposti ulteriori requisiti.[285]

Anche se si ritiene auspicabile che i pittogrammi utilizzati possano essere elaborati automaticamente, si respinge una leggibilità elettronica obbligatoria. Dopotutto, i pittogrammi dovrebbero principalmente fungere da orientamento e aumentare il livello di trasparenza. In questo senso, è d'importanza centrale semplificare il loro uso per le imprese. La leggibilità elettronica, tuttavia, aumenta gli ostacoli all'uso dei pittogrammi[286], tanto più che il regolamento è concepito come una concretizzazione dell'obbligo di informare, soggetto a sanzioni penali[287]. Ciononostante, secondo SWICO, non è definitivamente chiaro se una violazione del capoverso sia punibile.

Inoltre è poco chiaro cosa si debba intendere per «leggibilità a macchina».[288] Ciò potrebbe creare incertezza giuridica, che impedirebbe ulteriormente l'uso dei pittogrammi.[289] Non ci sono

[277] Organizzazione: ASB.

[278] Organizzazioni: economiesuisse, ASB, VUD.

[279] Organizzazioni: Curafutura, proFonds, SUISA.

[280] Cantone: SO; partiti: PLR.

[281] Organizzazioni: ABES, auto schweiz, Datenschutzguide.ch, ASA.

[282] Organizzazioni: EXPERTsuisse, IGEM, suva, swissICT, VUD, Walderwyss.

[283] Partiti: PLR; organizzazioni: Datenschutzguide.ch, EXPERTsuisse, IGEM, Migros, USI, SPA, SWICO, swissICT.

[284] Organizzazioni: economiesuisse, Privacy Icons, ASB, VUD.

[285] Organizzazioni: la Posta, economiesuisse, IGEM, ASB, ASSL, suva.

[286] Organizzazioni: Migros, ASB (per analogia), SWICO, VUD, Walderwyss.

[287] Organizzazione: Migros.

[288] Organizzazioni: ABES, UPSA, economiesuisse, CFC, FER, ASB, ASSL, SPA, SWICO, suva, ASA, VUD.

[289] Organizzazioni: Curafutura, DFS, economiesuisse, Migros, Privacy Icons, ASB, VUD.

nemmeno standard per queste indicazioni.[290] Secondo santésuisse non è neppure chiara la relazione tra pittogrammi e «leggibilità a macchina».

C'è anche un errore di ragionamento. Lo scopo dei pittogrammi è quello di veicolare informazioni più facilmente che un testo e di permettere alle persone di reagire intuitivamente a una dichiarazione sulla protezione dei dati. Se, invece, una dichiarazione sulla protezione dei dati deve essere valutata in modo automatico, dovrebbe essere leggibile elettronicamente la dichiarazione stessa e non i pittogrammi o il suo contenuto andrebbe codificato di conseguenza.[291]

Si chiede di stralciare la disposizione. Se la disposizione non dovesse essere stralciata interamente, il testo dovrebbe almeno chiarire che non andrebbero imposti requisiti così elevati per la leggibilità elettronica. In tal senso, dovrebbe essere sufficiente, per esempio, fornire un testo esplicativo per i file di immagini o formattare i pittogrammi come scrittura[292] di modo che possano essere elaborati da un computer.[293] L'ASDPO osserva che andrebbero date ulteriori spiegazioni se la disposizione dovesse essere mantenuta. Per esempio, in quali contesti e che tipo di pittogrammi verrebbero usati o se dovrebbero essere riconosciuti dall'IFPDT.

La Posta accoglierebbe con favore il chiarimento, in linea con l'articolo 13 RGPD, che gli obblighi di informazione non richiedono l'indicazione degli Stati di destinazione per le trasmissioni all'estero. Invece, nel caso di Stati di destinazione non sicuri i Paesi a cui i dati sono comunicati e le garanzie applicabili dovrebbero essere determinabili per gli interessati sulla base delle informazioni fornite.

3.2.14 Art. 14 AP-OLPD: Obbligo di informare degli organi federali nell'ambito della raccolta sistematica di dati personali

Si osserva che il carattere facoltativo dell'informazione si applica anche in casi diversi dall'uso di un questionario. Ciò andrebbe indicato più chiaramente nella norma[294]. Alcuni osservano anche che l'obbligo di fare riferimento al carattere volontario dovrebbe sussistere solo se non risulta chiaramente dalle circostanze[295]. Infine, swissICT critica la confusione tra la protezione dei dati e gli obblighi legali di cooperazione. Tuttavia, la protezione dei dati è rilevante indipendentemente dal fatto che le informazioni vadano fornite volontariamente o obbligatoriamente.

3.2.15 Art. 15 AP-OLPD: Informazione in occasione della comunicazione di dati personali

La norma è esplicitamente approvata da FRC, ma riceve anche alcune critiche. Manca una base legale che andrebbe disciplinata nella legge[296]. Più precisamente, il Parlamento ha già disciplinato chiaramente la comunicazione dei dati personali a livello di legge in diversi punti, ma basandosi su principi e rischi. Inoltre, ha voluto creare un adeguato potere discrezionale per l'attuazione individuale da parte dei singoli responsabili.[297]

---

[290] Organizzazioni: IGEM, suva, SWICO, swissICT, VUD.

[291] Organizzazioni: IGEM, suva VUD.

[292] Webfont.

[293] Organizzazioni: economiesuisse, Privacy Icons, ASB, VUD.

[294] Organizzazioni: ASDPO, HDC, swissprivacy.law.

[295] Organizzazioni: Curafutura, IGEM, FFS, SNP, suva, ASA, SWICO, VUD, Walderwyss.

[296] Cantone: LU; partiti: Alleanza del centro, PLR; organizzazioni: UPSA, auto schweiz, CP, curafutura, Datenschutzguide.ch, DFS, la Posta, economiesuisse, EXPERTsuisse, HDC, IGEM, Migros, EPS, pharmasuisse, proFonds, Rega, Ringier, santésuisse, ASB, Scienceindustries, SDV, usam, ASSL, SPA, SSO, UCS, suisa, suva, swissICT, Swiss Insights, swissstaffing, SWICO, veb.ch, vsi, VSP, UTP, VUD.

[297] Organizzazioni: Economiesuisse, ASB, Scienceindustries Switzerland.

La Posta osserva che l'articolo 15 OLPD contraddice l'articolo 19 capoverso 1 nLPD. pharmasuisse osserva che la nLPD impone solo l'obbligo di informare i destinatari su richiesta della persona interessata. Altri pareri sostengono che si applicano già i principi dell'articolo 6 nLPD, che stabilisce che chiunque tratti dati personali debba assicurarsi che siano corretti.[298]

Si osserva anche che l'articolo è superfluo, poiché il titolare del trattamento dei dati deve garantire il rispetto dei principi della protezione dei dati. In questo senso, l'informazione resta superflua nel caso del trattamento dei dati previsto dalla legge.[299] Inoltre, il destinatario ha l'obbligo di assicurarsi dell'esattezza dei dati e di rispettare i principi di trattamento. Una relativa informazione da parte di chi trasmette i dati pregiudicherebbe tale obbligo o rischierebbe di rendere una delle possibili misure di accertamento l'unico standard valido. Ciò è contrario alla legge.[300]

Inoltre, poiché un tale obbligo d'informazione per i privati non è previsto nel RGPD , si tratta di uno swiss finish.[301] Almeno nel settore privato, non andrebbe fatto riferimento alla direttiva [UE] 2016/680. L'articolo 7 paragrafo 2 della direttiva si riferisce chiaramente alle «autorità competenti».[302] Il disciplinamento andrebbe quindi almeno limitato agli organi federali.[303] Per quanto riguarda questa restrizione, tuttavia, le FFS, ad esempio, osservano che la direttiva [UE] 2016/680 si applica solo nel settore del diritto penale e non può essere usata come base legale in altri settori.

Il disciplinamento è anche considerato non in linea con la pratica,[304] poiché è sproporzionato e pieno di formalismi.[305] In termini di contenuto, si impongono requisiti aggiuntivi troppo severi per ogni tipo di comunicazione in relazione ai dati personali.[306] Ciò varrebbe anche nei casi in cui non vi fosse un rischio riconoscibile[307] e sarebbbe contrario agli sforzi del Consiglio federale di promuovere la digitalizzazione e l'innovazione nell'interesse della piazza economica svizzera.[308]

In particolare, si critica il fatto che i destinatari debbano ora essere aggiornati sulla completezza dei dati. Concretamente ciò significa che i dati comunicati non devono essere incompleti.[309] Altri osservano che nell'applicazione della disposizione, bisognerebbe evitare che il grado di dettaglio delle informazioni associate alla comunicazione sia troppo ampio.[310] Altri ancora pensano che la norma andrebbe limitata ai dati il cui trattamento pone un rischio residuo.[311]

[298] Cantone: BE; organizzazioni: Bär & Karrer, proFonds, suva, swissICT.

[299] Organizzazioni: UPSA, curafutura, Rega, ASSL, ASA, UTP, VUD.

[300] Organizzazioni: H+, IGEM.

[301] Organizzazioni: UPSA, Digitialswitzerland, Economiesuisse, EXPERTsuisse, HotellerieSuisse, IGEM, Ringier, USI, ASB, Scienceindustries Switzerland, ASSL, suva, SWICO, SwissHoldings, VUD.

[302] Cantone: TG (implicito); organizzazioni: UPSA, economiesuisse, HotellerieSuisse, ASSL.

[303] Organizzazioni: economiesuisse, EXPERTsuisse, ASB.

[304] Organizzazioni: DFS, HÄRTIG Rechtsanwälte, H+, IGEM, Migros, SDV, suva, ASA, SwissHoldings, swissICT.

[305] Organizzazioni: CP, SDV.

[306] Organizzazioni: CP, curafutura, la Posta, economiesuisse, IGEM, Rega, ASB, suva, SwissHoldings, swissICT, VUD.

[307] Organizzazione: CP.

[308] HDC, SwissHoldings.

[309] Organizzazioni: la Posta, H+, IGEM, suva, veb.ch.

[310] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex.

[311] Organizzazioni: HDC, SwissHoldings.

Come minimo andrebbe stralciato il responsabile del trattamento, dato che gli obblighi di informazione secondo la nLPD non si applicano a quest'ultimo.[312] Inoltre, spesso il responsabile stesso non è in possesso delle informazioni necessarie.[313] In definitiva, secondo SWICO, è responsabilità del titolare dei dati garantire il rispetto dei principi di protezione dei dati.

Infine, il forum PMI ritiene il disciplinamento troppo impreciso e bisognoso di interpretazione. SPA osserva che non è chiaro cosa si intenda per «affidabilità» dei dati personali.

3.2.16 Art. 16 AP-OLPD: Informazione sulla rettifica, sulla cancellazione o la distruzione nonché sulla restrizione del trattamento di dati personali

Due partecipanti alla consultazione sono dell'opinione che la norma non sia abbastanza ampia. È di fondamentale importanza che la persona interessata sia informata immediatamente sulla rettifica, cancellazione o distruzione dei suoi dati.[314] D'altra parte, si nota che gli obblighi previsti dall'articolo 16 AP-OLPD erano già inclusi nel progetto della nLPD e sono stati esplicitamente respinti dal Parlamento.[315] In questo senso, non vi è nemmeno una base legale.[316] Inoltre, il diritto della persona interessata alla «limitazione» del trattamento allude all'articolo 18 del RGPD e non esiste nella nLPD.[317] Inoltre, la rettifica, la cancellazione, la distruzione e la restrizione del trattamento dei dati personali avvengono nell'interesse della persona interessata.[318] Il titolare deve comunque rispettare i principi di trattamento o assicurarsi che vengano rispettati.[319]

Oltre a questo rifiuto fondamentale della norma per la mancanza di una base legale o la ridondanza della norma stessa, vi sono anche commenti più dettagliati. HDC osserva che gli obblighi previsti andrebbero limitati nel tempo. Andrebbe anche chiarito che non può essere un obbligo del titolare quello di conservare per il destinatario una copia dei dati trasmessi. UPSC nota che l'espressione «onere sproporzionato» andrebbe descritta più precisamente nel rapporto esplicativo o nell'ordinanza stessa. Il margine di interpretazione è troppo ampio e si crea la possibilità di fare a meno di tali informazioni al fine di evitare sforzi. DigiGes osserva che la norma non solleva i titolari del trattamento dei dati dal loro dovere di informare le persone interessate. Questo va specificato.

3.2.17 Art. 17 AP-OLPD: Riesame di una decisione individuale automatizzata

L'articolo è accolto con favore da molti partecipanti. Si sottolinea, che una decisione automatizzata può portare a inequità.[320] La norma intende giustamente evitare che le persone interessate esitino a richiedere tale revisione. Altri partecipanti sono critici. Il Parlamento ha già disciplinato gli obblighi d'informazione per le decisioni individuali automatizzate nell'articolo 21 nLPD in modo sufficientemente chiaro, ma comunque basato su principi e rischi. Inoltre, ha voluto deliberatamente fornire un adeguato potere discrezionale per l'attuazione individuale da parte del singolo titolare. Ulteriori indicazioni che potrebbero essere desunte dal progetto

[312] Cantone: BE; organizzazioni: Curafutura, FMH, pro Fonds, santésuisse, SDV, UCS, SWICO, swissstaffing, VUD.

[313] Organizzazioni: IGEM, UCS, suva, swissICT, VUD.

[314] Organizzazioni: FRC, DigiGes.

[315] Cantone: BE; partiti: Alleanza del centro, PLR; organizzazioni: UPSA, economiesuisse, HotellerieSuisse, proFonds, Rega, ASB, usam, ASSL, UCS, suisa, Swiss Insights, veb.ch, VUD.

[316] Cantone: BE; partiti: Alleanza del centro, PLR; organizzazioni: UPSA, Creditreform, curafutura, HotellerieSuisse, proFonds, ASSL, SSO, suisa, Swiss Insights, UTP.

[317] Organizzazioni: HotellerieSuisse, Rega, VUD.

[318] Organizzazioni: Creditreform, UTP.

[319] Organizzazioni: UPSA, Creditreform, ASSL, Swiss Insights, UTP.

[320] Partiti: SP; organizzazioni: USS, FRC.

non hanno una base legale.[321] Secondo alcuni, l'articolo interviene anche sull'autonomia privata e va quindi sancito dalla legge.[322]

Inoltre, il regolamento si basa su premesse legali errate. Non esiste un divieto generale di discriminazione. Se dovesse derivare direttamente dai diritti fondamentali della Costituzione, ciò è inammissibile, poiché non vi è un effetto diretto su terzi dei diritti costituzionali. La discriminazione diventa giuridicamente critica solo se è puramente soggettiva e senza criteri di delimitazione oggettivamente convincenti.[323] Secondo il Cantone di Lucerna, va discussa anche la conformità del disciplinamento con la legge, poiché l'articolo 61 della legge prevede una disposizione sulla responsabilità penale.

Asut sostiene che non è chiaro come debba essere intesa la frase «non deve essere svantaggiata». Il Forum per la protezione dei dati vorrebbe vedere i possibili svantaggi elencati a titolo di esempio. L'Associazionedicommercio.swiss ritiene che questa frase non sia realisticamente attuabile. Nella maggior parte dei casi, la persona interessata si sente svantaggiata dalla messa in discussione della decisione individuale automatizzata. Inoltre, i fornitori sono autorizzati a scegliere i loro partner contrattuali. Tuttavia, questa norma è anche espressamente approvata. È importante evitare il più possibile la discriminazione nelle decisioni individuali automatizzate. In questo senso, è positivo che il Consiglio federale fissi nell'ordinanza esecutiva che chi chiede il riesame di una decisione individuale automatizzata da parte di una persona fisica non debbano esserne svantaggiati.[324]

HDC è del parere che il divieto di discriminazione previsto dall'articolo 17 AP-OLPD vada concretizzato. L'autorità di protezione dei dati del Cantone di Friburgo osserva anche che non è chiaro se una richiesta di riesame ai sensi dell'articolo 17 AP-OLPD possa portare a una nuova decisione. Il Cantone di San Gallo osserva che la disposizione dovrebbe precisare che le decisioni individuali automatizzate non dovrebbero esplicare effetto fino all'attestato di verifica.

In generale, si osserva che un tale disciplinamento incoraggerebbe le cause abusive contro i titolari del trattamento.[325] Inoltre, niente di tutto questo andrebbe regolato nell'AP-OLPD, poiché l'argomento è di natura generale e gioca un ruolo altrettanto importante in tutte le materie legali. Solo la prassi consolidata del Tribunale federale fornisce sufficiente certezza del diritto.[326]

USS vede un pericolo reale che sempre più decisioni siano automatizzate nel campo dell'occupazione e chiede una migliore protezione dal licenziamento (aumento dell'indennità a 24 mesi e diritto alla reintegrazione nell'art. 336*a* CO).

3.2.18 Art. 18 AP-OLPD: Forma e conservazione della valutazione d'impatto sulla protezione dei dati

Il PS accoglie con favore il termine di conservazione proposto dal Consiglio federale e chiede esplicitamente che tale termine non sia ridotto. Il DFS vorrebbe che il termine di conservazione fosse esteso a cinque anni, adducendo che la valutazione d'impatto sulla protezione dei dati è uno strumento estremamente utile per il contenimento sistematico dei rischi e rappresenta una delle innovazioni più importanti della nLPD. Se la persona interessata subisce un danno a causa di un trattamento improprio dei dati e in seguito sorgono questioni di responsabilità,

[321] Cantone: Lucerna; organizzazioni: Economiesuisse, asut.

[322] Organizzazioni: Bär & Karrer (per analogia), economiesuisse, ASB.

[323] Organizzazioni: Bär & Karrer (per analogia), economiesuisse, ASB.

[324] Partiti: PS, organizzazioni: FRC, USS.

[325] Organizzazioni: economiesuisse, ASB, swissICT.

[326] Organizzazioni: economiesuisse, ASB.

la valutazione d'impatto sulla protezione dei dati può servire come documento per esaminare eventuali rivendicazioni di diritti. ASDPO trova discutibile che i termini di conservazione nell'AP-OLPD non siano armonizzati e propone anch'essa un periodo di 5 anni. Bär & Karrer trova incomprensibile la definizione dei termini di conservazione e vorrebbe termini uniformi per semplificare il compito alle imprese.

Altri pareri sono critici. Si critica che l'obbligo di conservazione per la valutazione d'impatto sulla protezione dei dati non ha una base legale. Tale obbligo generale di documentazione è stato deliberatamente omesso nella nLPD in favore dell'obbligo di tenere un registro delle attività di trattamento.[327] Il Cantone di Svitto osserva che la valutazione d'impatto sulla protezione dei dati per gli organi federali, in quanto documento ufficiale, dovrebbe essere soggetta alle regole generali sull'obbligo di conservazione dei documenti e non disciplinata separatamente nella OLPD. Si critica anche che si tratta di uno swiss finish, dato che il RGPD non prevede un tale obbligo.[328]

Inoltre, la conservazione contraddice il principio del nemo tenetur[329], poiché la valutazione d'impatto sulla protezione dei dati conservata potrebbe essere usata come prova contro il titolare prima di o nel contesto di una controversia legale basata su una richiesta di pubblicazione.[330]

Si suggerisce almeno un accorciamento del termine. Quest'ultimo è ritenuto troppo lungo,[331] soprattutto perché il trattamento dei dati secondo l'articolo 5 lettera d nLPD comprende anche l'archiviazione.[332] Alcuni partecipanti ritengono inoltre che, in virtù del principio di proporzionalità del trattamento dei dati e della minimizzazione dei dati, non sussiste alcuna ragione che giustifichi un termine di conservazione così lungo.[333] Inoltre, il Cantone di Zurigo osserva da un lato che i risultati della valutazione d'impatto sulla protezione dei dati confluirebbero direttamente nel trattamento dei dati valutato e, dall'altro, che, trattandosi di una valutazione istantanea, diventerebbe molto rapidamente obsoleta. Alcuni partecipanti suggeriscono che il termine di conservazione duri al massimo fino alla fine del trattamento dei dati considerato, poiché in seguito non è più possibile alcuna violazione dei diritti della persona interessata.[334] Asut suggerisce anche che spetti al titolare dei dati definire la durata del termine di conservazione in modo adeguato per ogni singolo caso, tenendo conto dell'obbligo di fornire prove. Infine, si desidera una graduazione secondo la necessità di protezione dei dati.[335] Se il termine fosse mantenuto, andrebbe precisato che la conservazione dovrebbe durare «almeno» due anni, di modo che una conservazione più lunga non andasse contro la legislazione sulla protezione dei dati.[336]

[327] Organizzazioni: ABES, UPSA, Bär & Karrer, CP, Creditreform, economiesuisse, HÄRTING Rechtsanwälte, HotellerieSuisse, IGEM, Migros, EPS, pharmasuisse, FSA, ASB, usam, ASSL, BNS, SPA, UCS, suisa, suva, swissICT, swissstaffing, vsi, VSP, VUD, Walderwyss.

[328] Organizzazioni: UPSA, Migros, ASSL.

[329] Secondo il principio nemo tenetur, nessuno è tenuto ad accusare o incriminare se stesso. Il principio nemo tenetur è ritenuto il principio fondamentale di un equo procedimento penale.

[330] Organizzazioni: economiesuisse, ASB.

[331] Cantone: ZH; organizzazioni: IS, ASPS, Curaviva Schweiz, Creditreform, INSOS, EPS, ASP, senesuisse, Spitex Schweiz, VSP.

[332] Organizzazione: swissprivacy.law.

[333] Organizzazioni: economiesuisse, ASB.

[334] Organizzazioni: Creditreform, EPS, ASP, VSP.

[335] Organizzazioni: Classtime, vsi.

[336] Organizzazioni: economiesuisse, BNS, Walderwyss.

Inoltre, si desidera che sia esplicitamente menzionato nell'ordinanza[337] che la forma scritta può includere anche altre forme - elettroniche - che permettono la prova per testo. Non basta menzionarlo solo nel rapporto esplicativo.[338] Si critica il fatto che la forma scritta vada intesa nel senso del CO e richieda quindi una firma (TAF A-3548/2018 del 19 marzo 2019, consid. 4.8.4). Dovrebbe quindi essere possibile preparare e conservare la valutazione d'impatto sulla protezione dei dati in forma elettronica, a condizione che sia conservata in modo sicuro e possa essere consultata immediatamente in qualsiasi momento.[339] La forma scritta non è né necessaria né al passo coi tempi.[340] Altri pensano che non sia chiaro se un semplice messaggio elettronico basti a soddisfare il requisito della forma scritta o se sia necessaria una firma elettronica. Questo andrebbe specificato meglio. Tuttavia, i requisiti della forma scritta non dovrebbero essere troppo severi.[341] Se fosse mantenuto, il criterio della forma scritta andrebbe esplicitamente definito in modo più ampio rispetto al requisito formale dell'articolo 12 e seguenti CO.[342]

Più in dettaglio, si critica il fatto che il disciplinamento presuppone che la valutazione d'impatto sulla protezione dei dati non viene mai rinnovata. Questo non corrisponde alla pratica. Non è quindi chiaro come comportarsi con più versioni. Questo andrebbe chiarito facendo riferimento alla versione più recente.[343] Curafutura chiede che gli organi federali non siano tenuti ad effettuare una valutazione d'impatto sulla protezione dei dati se i dati sono trattati come previsto dalla legge. FMH ritiene che questa disposizione dovrebbe definire in modo più preciso la formulazione dell'articolo 22 capoverso 2 lettera a nLPD al fine di determinare inequivocabilmente cosa si intenda per «trattamento su larga scala».

3.2.19 Art. 19 AP-OLPD: Notifica di violazioni della sicurezza dei dati

Cpv. 1

Si osserva che l'articolo 24 capoverso 1 nLPD prevede la notifica delle violazioni della sicurezza dei dati solo se è probabile che vi sia un rischio elevato per la personalità e i diritti fondamentali della persona interessata. In questo senso, l'articolo 24 nLPD è una disposizione che si discosta deliberatamente dall'articolo 33 RGPD. Tuttavia, la maggior parte delle disposizioni dell'articolo 19 AP-OLPD sono state riprese dall'articolo 33 RGPD. Esse servirebbero principalmente ai titolari soggetti anche al RGPD. Secondo altri, sono disposizioni aggiuntive non necessarie che generano lavoro supplementare.[344] In particolare, l'indicazione del tempo e della durata della violazione va oltre il RGPD. Si tratta anche qui di uno swiss finish.[345] DigiGes sottolinea, invece, che l'indicazione del tempo e della durata non supera i limiti posti dalla legge. In primo luogo, l'indicazione dovrebbe avvenire solo se il tempo e la durata possono essere determinati e, in secondo luogo, solo se l'informazione è di fondamentale importanza

[337] Non solo nel rapporto esplicativo.

[338] Cantone: BE; organizzazioni: ABES, UPSA, ASDPO, Bär & Karrer, curafutura, DFS, la Posta, economiesuisse, FER, HÄRTING Rechtsanwälte, HotellerieSuisse, proFonds, Ringier, ASB, ASSL, BNS, SPA, suva, ASA, swissICT, swissprivacy.law, vsi, VUD, Walderwyss.

[339] Organizzazioni: ASDPO, curafutura, HDC, proFonds, swissprivacy.law, Walderwyss.

[340] Organizzazioni: asut, curafutura, ASA, swissprivacy.law.

[341] Organizzazioni: asut, Bär & Karrer, ASSOCIAZIONE DI COMMERCIO.swiss, santésuisse.

[342] Organizzazioni: HDC, swissprivacy.law.

[343] Organizzazioni: IGEM, BNS, suva, VUD, Walderwyss.

[344] Cantone: UR, AR, AG, BL, GR, NW, SH, SZ, VD, ZH; organizzazioni: responsabile della protezione dei dati SZ/OW/NW, privatim.

[345] Organizzazioni: UPSA, auto schweiz, ASB, ASSL, Digitalswitzerland, Ringier, suva, Swiss Insights.

per poter valutare la portata della violazione. Suva ritiene anche che la lettera a vada oltre il RGPD. Tuttavia, questo non dovrebbe rappresentare un problema nella pratica.[346]

Altri obblighi vanno oltre l'articolo 24 capoverso 4 nLPD. I criteri delle lettere b-d non possono essere dedotti dalla legge. Non sussiste in proposito alcuna base legale.[347] L'indebolimento di molte di queste disposizioni aggiuntive con l'aggiunta di «se possibile» è di scarsa utilità. L'obiettivo è che l'autorità di controllo sia informata rapidamente, e se necessario anche le persone interessate, e che le misure di protezione dei dati personali siano adottate immediatamente. Pertanto, la precisazione nell'articolo 19 dell'AP-OLPD non è necessaria.[348] Altri partecipanti trovano l'aggiunta utile, poiché le indicazioni spesso non sono attuabili nella pratica.[349] DigiGes afferma che le informazioni di cui alle lettere a-g sono necessarie affinché l'IFPDT possa farsi un quadro completo nei casi di violazione della sicurezza dei dati. Ciò è sottolineato anche nel rapporto esplicativo. ASDPO sottolinea che le informazioni alle lettere b-d vanno fornite in ogni caso e che l'aggiunta di «se possibile» andrebbe cancellata.

Asut osserva che le lettere e ed f sono formulate in modo poco chiaro e non indicano il fatto che vanno segnalate all'IFPDT solo le violazioni che «possono comportare un rischio elevato per la personalità o i diritti fondamentali della persona interessata».[350] Vi è inoltre l'opinione che la lettera e dovrebbe recitare «le conseguenze che rappresentano un rischio elevato per le persone interessate». Questo include già tutti i possibili rischi.[351] Inoltre, si osserva che l'articolo 33 capoverso 3 lettera c del RGPD parla di «probabili conseguenze». Questa formulazione dovrebbe essere adottata anche per l'AP-OLPD, poiché in pratica il titolare può solo fare una stima delle conseguenze.[352] Altri partecipanti chiedono che la lettera e includa anche l'aggiunta «se possibile», poiché non è sempre possibile determinare immediatamente e definitivamente le conseguenze e i possibili rischi non appena viene scoperta una violazione della sicurezza dei dati.[353] Inoltre, la lettera f dovrebbe parlare di «rischio» e non di «conseguenze».[354] SwissICT sottolinea che anche se si è rimediato a un difetto, bisogna cionostante mitigare le conseguenze o i danni.[355] Economiesuisse sottolinea inoltre che andrebbe indicato tramite l'espressione «se del caso» che sono da segnalare solo le misure effettivamente adottate.

swissprivacy.law chiede di chiarire che vanno notificate tutte le informazioni solo in caso di obbligo di notifica. Se l'IFPDT è informato volontariamente, non devono essere forniti tutti i dati elencati al capoverso 1. Si chiede anche un regolamento «de minimis», che esclude i casi in cui l'IFPDT non ha la possibilità di agire. Ciò permetterebbe di risparmiare risorse.[356]

[346] Organizzazioni: ASB, suva.

[347] Cantone: BS; organizzazioni: Creditreform, ASSOCIAZIONE DI COMMERCIO.swiss, Ringier, ASP, usam, SPA, vsi, VSP.

[348] Cantone: AG, AR, BS, BL, GR, NW, OW, SH, VD, ZH; organizzazioni: privatim.

[349] Organizzazioni: economiesuisse, ASB, SPA.

[350] Altrettanto l'organizzazione: HÄRTING Rechtsanwälte.

[351] Organizzazioni: economiesuisse, IGEM, SPA, suva, swissICT.

[352] Organizzazioni: FER, HANDELSVERBAND.swiss.

[353] Organizzazioni: Creditreform, ASSOCIAZIONE DI COMMERCIO.swiss, ASP, usam, vsi, VSP.

[354] Organizzazioni: economiesuisse, ASB, SPA.

[355] Anche l'organizzazione: HÄRTING Rechtsanwälte.

[356] Organizzazioni: economiesuisse, IGEM, ASB, SPA, suva, VUD.

Cpv. 2

L'indicazione «al momento della scoperta della violazione della sicurezza dei dati» non sembra avere molto senso. L'esperienza mostra che in tale momento il titolare del trattamento non possiede ancora tutte le informazioni necessarie, poiché richiedono tempo per essere raccolte.[357] ASDPO, d'altra parte, sottolinea che va chiaramente indicato che le informazioni vanno rese disponibili il prima possibile e non solo al momento della scoperta della violazione.

Cpv. 3

Alcuni partecipanti sottolineano che la legge impone di fornire informazioni alla persona interessata solo se ciò è necessario per la sua protezione o se l'IFPDT lo richiede. Al contrario, l'ordinanza prevede sempre la comunicazione di informazioni di cui al capoverso 1 lettere a, e, f e g. Non vi è quindi alcuna base legale.[358] Pertanto, secondo FER, andrebbe chiarito che questa disposizione si applica solo se la legge prevede che la persona interessata vada informata.[359] Al contrario, il PS vuole che il tempo e la durata della violazione siano comunicati anche alla persona interessata, così che possa valutare al meglio la portata e il rischio della violazione. ASDPO vorrebbe inoltre che alla persona interessata siano comunicate le informazioni di cui alle lettere b e c. Questo potrebbe aiutare a determinare la portata dell'incidente e ad adottare le misure appropriate.[360] Altri suggeriscono di omettere la lettera g, poiché facilita gli attacchi informatici o poiché nelle imprese più grandi non c'è una sola persona di contatto.[361]

Cpv. 4

HDC sottolinea che l'articolo 24 capoverso 6 nLPD prevede che una notifica può essere usata contro la persona soggetta all'obbligo di notifica in un procedimento penale solo con il suo consenso. Si dovrebbe quindi chiarire che nel caso di una persona giuridica, la disposizione prevede l'obbligo di notifica per la persona giuridica in quanto tale e per qualsiasi persona fisica all'interno della persona giuridica. Il Cantone di Friburgo sottolinea che bisogna evitare che ogni notifica sia resa pubblica prematuramente. Tuttavia, il Tribunale federale ha stabilito che una notifica sulle violazioni della sicurezza dei dati è soggetta al principio della trasparenza (DTF 1C_500/2020 dell'11 marzo 2021). Poiché questa notifica diventa ora obbligatoria, è opportuno prevedere un limite di tempo per la consultazione di tali notifiche.

Cpv. 5

DigiGes sottolinea che è importante per tutte le parti coinvolte che la violazione sia documentata, come previsto dall'articolo 19 capoverso 5. ASDPO ritiene che sarebbe utile se tutte le violazioni fossero notificate, in modo che l'IFPDT o altre autorità possano verificare in caso di ispezione se non è stata notificata una violazione da notificare. Alcuni partecipanti ritengono che non sia chiaro se tutte le violazioni vadano documentate o solo quelle che devono essere notificate all'IFPDT.[362] Altri, tuttavia, credono fermamente che andrebbero documentate solo le

[357] Organizzazioni: IGEM, santésuisse, suva, VUD.

[358] Organizzazioni: UPSA, asut, auto Swiss, economiesuisse, FER, ASSOCIAZIONE DI COMMERCIO.swiss, ASP, ASSL, SPA, Swiss Insights, vsi VSP.

[359] Organizzazione: FER.

[360] Anche l'organizzazione: Swimag (per analogia).

[361] Organizzazioni: ABES, swissICT.

[362] Organizzazioni: ASDPO, swissprivacy.law.

violazioni soggette all'obbligo di notifica. Per questo motivo, lo scopo della norma risulta poco chiaro, dato che l'IFPDT farebbe comunque richiesta se ve ne fosse l'interesse.[363]

Molti partecipanti chiedono che l'obbligo di documentazione di cui al capoverso 5 sia cancellato, poiché manca di una base legale.[364] L'obbligo di notificare le violazioni della sicurezza dei dati è già sufficientemente chiaro nella legge ed è comunque disciplinato sulla base di principi e rischi. Di conseguenza, il Parlamento ha voluto deliberatamente fornire un margine di discrezione adeguato per l'attuazione individuale da parte del singolo titolare del trattamento.[365] L'articolo 24 nLPD non contiene un obbligo di documentare e conservare le informazioni in relazione a una violazione della sicurezza.[366] Ciò non è previsto nemmeno dal RGPD. Si tratta anche qui di uno swiss finish.[367]

Inoltre, si critica il fatto che l'obbligo è troppo severo, poiché tutti i «fatti legati agli eventi» andrebbero documentati.[368] L'espressione «fatti legati» suggerirebbe erroneamente che per l'obbligo di documentazione andrebbero indagati fatti non elencati secondo il capoverso 1 lettere a-g.[369] ABES sottolinea che se la norma fosse mantenuta, dovrebbe essere specificato che il titolare deve solo mettere a disposizione informazioni che sono note. Non ci si può aspettare che le indagini siano effettuate presso esterni.

Molti partecipanti chiedono di accorciare il termine di conservazione.[370] Alcuni sostengono che la documentazione dovrebbe essere conservata in conformità con le disposizioni di conservazione applicabili alle autorità di vigilanza.[371] Altri vorrebbero che i termini di conservazione fossero uniformati in tutta l'ordinanza, e quindi anche in questo articolo.[372] Altri ritengono che il termine di conservazione vada esteso a cinque anni, poiché la notifica potrebbe essere rilevante in caso di rivendicazioni di responsabilità.[373] DigiGes sottolinea l'importanza del periodo di conservazione per la persona interessata, poiché le permette di opporsi per vie legali. Economiesuisse chiede che venga chiarito che devono essere conservate solo le violazioni soggette all'obbligo di notifica.

Infine, si critica il fatto che il rapporto esplicativo definisce in modo errato il termine «verosimilmente» quando afferma che una notifica deve essere effettuata anche «nei casi dubbi, in cui non si può escludere un rischio elevato». Questo presuppone che una violazione della sicurezza dei dati porterebbe molto probabilmente a un rischio elevato.[374] Tuttavia, questo è un pleonasmo. Il termine «rischio» include già una considerazione sulla probabilità che si verifichi un danno. Pertanto, la probabilità deve essere di una certa portata.[375] Il termine «verosimilmente» non significa affatto che la notifica debba essere effettuata in ogni «caso dubbio»

[363] Organizzazioni: H+, HDC, Rega, BNS, suva, SWICO.

[364] Organizzazioni: ABES, UPSA, asut, auto schweiz, Bär & Karrer, Creditreform, economiesuisse, EXPERTsuisse, H+, ASSOCIAZIONE DI COMMERCIO.swiss, IGEM, Migros, pharmasuisse, Rega, ASP, FSA, ASB, Scienceindustries, sgv, ASSL, BNS, SPA, UCS, suisa, suva, SWICO, SwissHoldings, swissICT, swissprivacy.law, swissstaffing, veb.ch, VSP, VUD, vsi, Walderwyss.

[365] Organizzazione: ASB.

[366] Organizzazioni: HDC, Rega.

[367] Organizzazioni: UPSA, auto schweiz, Digitalswitzerland, Migros, Scienceindustries, ASSL, Swiss Insights, SwissHoldings.

[368] Organizzazioni: Bär & Karrer, proFonds.

[369] p. es. organizzazioni: Bär & Karrer, suva. Ritenuto un concetto poco chiaro da Walderwyss.

[370] Organizzazioni: Creditreform, curafutura, proFonds, Ringier, ASP, santésuisse, ASA, vsi, VSP, Walderwyss.

[371] Cantone: ZH; organizzazioni: usam.

[372] Organizzazioni: Bär & Karrer, curafutura, FMH, Ringier, ASA, Walderwyss.

[373] Organizzazioni: ASDPO, DFS, Swimag.

[374] E non che «nei casi dubbi, in cui non si può escludere un rischio elevato, deve essere effettuata una notifica». Organizzazioni: Auto Schweiz, economiesuisse, ASB, vsi.

[375] Organizzazioni: IGEM, ASB, suva, VUD.

in cui non si può escludere un rischio elevato. Piuttosto, va effettuata solo se il rischio di una violazione dei diritti della persona interessata è chiaramente superiore alla probabilità che non si verifichi alcuna violazione.[376] Concretamente, si intendono casi in cui la violazione della sicurezza dei dati porterebbe con tutta probabilità a un rischio elevato.[377] Il Consiglio federale supera qui i limiti fissati dal legislatore.[378] FMH vorrebbe che le spiegazioni sul termine «verosimilmente» fossero integrate nell'ordinanza.

3.2.20 Art. 20 AP-OLPD: Modalità

Diversi partecipanti considerano positivo che il diritto d'informazione dei privati sia rafforzato nell'AP-OLPD. Il diritto d'informazione è un principio essenziale della protezione dei dati.[379] La Fondazione per la protezione dei consumatori nota che senza informazioni, gli interessati non potrebbero sapere quali dati che li riguardano vengono elaborati. In questo senso, il diritto d'informazione andrebbe limitato il meno possibile[380] e disciplinato in modo tale che sia possibile per la persona interessata esercitare questo diritto a intervalli appropriati.[381] È altresì importante che questo diritto non sia usato in modo improprio.[382]

Altri pareri notano che l'articolo non porta alcun valore aggiunto, poiché l'articolo 25 nLPD e l'articolo 26 nLPD disciplinano già in dettaglio il diritto d'informazione e le sue restrizioni. Le concretizzazioni contenute nell'articolo 20 AP-OLPD sono superflue.[383] Si osserva anche che la portata e lo scopo dell'informazione si evincono già dall'articolo 25 capoverso 2 nLPD.[384]

Un altro punto generale è che si dovrebbe aggiungere che l'informazione, come descritta nel rapporto esplicativo, dovrebbe essere possibile anche in un'altra «forma verificabile per testo» - principalmente la forma elettronica.[385] Secondo HDC, il requisito della forma scritta non è giustificato in tutti i casi, poiché la forma elettronica di solito è sufficiente. Non è giustificato che il titolare richieda una firma scritta a mano in relazione alla richiesta di accesso. Anche se questo è menzionato nel rapporto esplicativo, sarebbe utile - per evitare incertezze nell'applicazione del diritto - specificarlo anche nell'ordinanza.[386] Inoltre, secondo la SPA, dovrebbe essere descritto più precisamente nel rapporto esplicativo se la «forma digitale» in quanto «forma elettronica» vada intesa nel senso di «per scritto». Questo è esplicitamente richiesto da Swimag e dovrebbe essere stabilito nell'ordinanza. Tuttavia, Creditreform nota a questo proposito che l'AP-OLPD non è esattamente il luogo ottimale per una tale «decisione di sistema».[387]

[376] Organizzazioni: UPSA, Creditreform, ASSL, Swiss Insights, vsi.

[377] Organizzazioni: economiesuisse, SPA.

[378] Organizzazioni: UPSA, Creditreform, ASSL, Swiss Insights, vsi.

[379] Partiti: I VERDI; organizzazioni: DigiGes, Fondazione per la protezione dei consumatori.

[380] Partito: I VERDI

[381] Organizzazioni: DFS, FRC.

[382] Organizzazione: DFS.

[383] Cantoni: AR, AG, ZH, UR, SH, VD; organizzazioni: privatim.

[384] Cantoni: AG, AI, AR, BS, GL, GR, NW, OW, SH, SZ, UR, VD, ZH; organizzazioni: VUD

[385] Cantone: SG; organizzazioni: UPSA, auto schweiz, Creditreform, HÄRTING Rechtsanwälte, ASSL, SPA, SWICO, Swiss Insights, swissstaffing, vsi, VUD.

[386] Cantone: SG, organizzazioni: economiesuisse, FER, HÄRTING Rechtsanwälte, SPA, SWICO, Swimag, swissICT, Swiss Insights, swissprivacy.law, vsi.

[387] Altrettanto l'organizzazione: vsi.

Cpv. 1

Numerosi partecipanti chiedono che una richiesta di informazioni sia possibile sia in forma scritta che orale. L'articolo 25 nLPD stabilisce solo che possono essere richieste «informazioni». Questo include sia la forma scritta che quella orale. Ciò significa che anche le persone per le quali la forma scritta rappresenta un ostacolo difficile o insormontabile posso richiedere informazioni. Far dipendere la forma della richiesta dal titolare potrebbe portare a decisioni arbitrarie.[388] SWICO osserva che questo non è molto utile nella pratica, in quanto una richiesta di informazioni può sempre essere fatta oralmente, ma il titolare non ha l'obbligo di rispondere. Al contrario, il Cantone di Turgovia vorrebbe che la richiesta fosse fatta esclusivamente per scritto, in modo da evitare malintesi e conflitti ed evitare un aumento massiccio delle richieste.

HDC osserva che il termine «domanda d'informazioni» non corrisponde al termine usato nella nLPD.

Cpv. 2

Diversi fornitori di assistenza sanitaria suggeriscono di includere dei chiarimenti sull'eventuale fornitura di informazioni per le persone particolarmente bisognose di assistenza.[389] Singoli partecipanti chiedono che la consultazione in loco sia possibile in ogni caso, indipendentemente da chi la propone.[390] SPA chiede di precisare che la consultazione in loco costituisce anche un valido adempimento dell'obbligo d'informazione del titolare se le informazioni scritte non possono essere ragionevolmente fornite a causa di interessi legittimi.

Il rapporto esplicativo precisa che in caso di consultazione in loco, l'interessato deve poter chiedere fotocopie di determinati atti del proprio dossier. Si osserva che, contrariamente a quanto affermato nel rapporto esplicativo, non esiste un diritto alla consegna di atti o documenti.[391] Al contrario, il legislatore ha limitato la comunicazione ai «dati personali trattati in quanto tali». Questo permette di fornire informazioni in forma aggregata, il che andrebbe dichiarato più precisamente nel rapporto esplicativo.[392] FMH, invece, sottolinea che l'ottenimento di fotocopie non può essere soggetto alla condizione di consultare i dossier sul posto. Dovrebbe infatti sempre essere possibile ottenere delle fotocopie. swissICT osserva anche che l'espressione «determinati atti» rende poco chiaro quali documenti possono essere copiati. HÄRTING Rechtsanwälte suggerisce che la disposizione sia modificata per permettere che le fotocopie siano «a pagamento».

Cpv. 3

Si nota che l'affermazione nel capoverso 3 che le informazioni devono essere «comprensibili» per la persona interessata è fuorviante e poco chiara, in quanto implica uno standard soggettivo basato sulle capacità della persona interessata, quando andrebbe invece applicato uno standard oggettivo.[393] Deve essere sufficiente che i dati siano preparati e presentati in modo ordinato e quindi comprensibili in buona fede.[394] Qualunque condizione aggiuntiva andrebbe

[388] Cantone: SO; partiti: I VERDI; organizzazioni: ASDPO, DigiGes.

[389] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

[390] Organizzazioni: ASDPO, swissprivacy.law.

[391] Organizzazioni: UPSA, economiesuisse, ASSL, swissICT, Swiss Payment Association.

[392] Organizzazioni: UPSA, economiesuisse, ASSL, Swiss Payment Association.

[393] Cantoni: AR, AG, BE, BS, GL, NW, SH, SZ, UR, VD, ZH; organizzazioni: Bär & Karrer, responsabile della protezione dei dati SZ/OW/NW, economiesuisse, CFC, IGEM, privatim, proFonds, USI, suva, SWICO, swissICT, Walderwyss.

[394] Organizzazioni: economiesuisse, ASB, suva, swissICT, VUD.

oltre il principio di proporzionalità e porterebbe a uno sforzo supplementare sproporzionato, che in certe circostanze renderebbe anche impossibile rispettare il termine di 30 giorni.[395] La conseguenza sarebbe che più informazioni su questa persona andrebbero trattate e il diritto d'informazione non potrebbe più essere integrato nei processi dei titolari come uno standard scontato del diritto in materia di protezione dei dati.[396] Il disciplinamento potrebbe anche essere frainteso nel senso che il titolare dovrebbe spiegare i set di dati o addirittura i processi associati e i modelli di business alla persona che richiede le informazioni. Ciò prolungherebbe «artificialmente» e senza una ragione oggettiva la procedura e quindi lo sforzo per il titolare.[397] Tuttavia, non esiste in proposito alcuna base legale.[398] Al contrario, l'articolo 25 capoverso 2 nLPD contiene già il contenuto dell'informazione.[399]

Pertanto, il capoverso andrebbe stralciato[400] o andrebbe richiesta esplicitamente una comprensione oggettiva, p. es. aggiungendo «generale».[401] Un altro suggerimento è quello di aggiungere le parole «secondo le capacità/lo stato cognitivi».[402] Un altro suggerimento è quello di far precedere le parole «comprensibile in linea di principio».[403] Si osserva anche che «comprensibile» dovrebbe essere specificato nel senso che le informazioni devono essere fornite in una lingua nazionale o in inglese.[404] Bär & Karrer chiede di precisare che il titolare del trattamento dei dati è tenuto a fornire solo le informazioni di cui all'articolo 25 capoversi 1 e 2 nLPD.

SWICO osserva che si tratta di uno swiss finish.

Cpv. 4

Alcuni partecipanti commentano che non è necessario menzionare al capoverso 4 che i dati personali vanno protetti dall'accesso di terzi non autorizzati. Ciò risulta dall'articolo 8 nLPD nonché dalle disposizioni del primo capitolo dell'AP-OLPD e della prima sezione dell'AP-OLPD. Il capoverso va quindi stralciato.[405]

Inoltre, non c'è una base legale per un vero e proprio obbligo di collaborazione dell'interessato.[406] Si chiede di chiarire che se l'interessato non collabora alla propria identificazione, si è autorizzati a negargli l'informazione.[407]

Inoltre, si chiede più in dettaglio di sostituire il termine «identificazione» con «autenticazione».[408]

[395] Organizzazioni: economiesuisse, IGEM, ASB, SPA, suva, VUD.

[396] Cantoni: AR, NW, SH, SZ, VD; organizzazioni: responsabile della protezione dei dati SZ/OW/NW, privatim.

[397] Organizzazioni: economiesuisse, ASB.

[398] Cantoni: ZH; organizzazioni: VUD

[399] Cantoni: AG, BS, GL, SH, UR, ZH.

[400] p. es. Cantoni: VD, ZH.

[401] Cantone: BE.

[402] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, usam, Spitex Svizzera.

[403] Organizzazioni: DFS, FSA, VUD.

[404] Organizzazioni: Curafutura, santésuisse.

[405] Cantoni: AG, AR, AI, GR, NW, OW, SH, SZ, VD, ZH; organizzazioni: responsabile della protezione dei dati SZ/OW/NW, privatim.

[406] Organizzazioni: IGEM, suva.

[407] Organizzazioni: IGEM, santésuisse, suva.

[408] Organizzazioni: IGEM, suva, VUD.

Cpv. 5

Molti partecipanti osservano che non esiste una base legale per l'obbligo di documentare il rifiuto, la restrizione o il differimento dell'informazione, che corrisponde all'obbligo di conservazione.[409] Singoli partecipanti rilevano anche che l'obbligo di conservazione contraddice la volontà del legislatore.[410] DigiGes ritiene invece che l'articolo 8 capoverso 3 nLPD autorizzi il Consiglio federale a emanare disposizioni sui requisiti minimi di sicurezza dei dati. La disposizione poggia quindi su una base legale. Infine, singoli partecipanti sostengono che si tratta di uno swiss finish, poiché il RGPD non prevede un tale obbligo di conservazione.[411]

In particolare, l'obbligo di conservare la documentazione di cui al capoverso 5 dà adito a critiche. L'articolo 26 capoverso 4 nLPD prevede già che il titolare del trattamento dei dati indichi il motivo per cui rifiuta, restringe o differisce l'informazione. Questo è sufficiente per far valere un'azione in giudizio.[412] La documentazione potrebbe essere ottenuta con una copia della lettera di risposta. Questo sarebbe sufficiente affinché l'interessato possa far valere i propri diritti.[413] In questo senso, il Cantone di Basilea Città osserva che il criterio della forma scritta per le informazioni andrebbe introdotto e che il periodo di conservazione andrebbe eliminato. Il Cantone di Glarona afferma che nel caso di organi federali, i motivi della restrizione andrebbero comunque indicati nella decisione. L'obbligo di documentare e conservare le informazioni deriva già dall'obbligo procedurale di registrazione agli atti.

Si afferma che l'articolo 20 capoverso 5 AP-OLPD, che va oltre l'articolo 26 capoverso 4 nLPD, comporterebbe solo oneri ulteriori, senza alcun effetto per quanto riguarda l'esercizio o l'applicazione del diritto d'informazione della persona interessata.[414] Inoltre, tale disciplinamento obbligherebbe il titolare a trattare e conservare più dati personali di quelli necessari per i suoi scopi commerciali.[415] Il disciplinamento è anche inutile nella misura in cui, a causa dell'onere della prova, sussiste comunque un interesse da parte del titolare del trattamento dei dati a poter fornire la prova delle informazioni.[416]

Alcuni partecipanti osservano che non è chiaro perché la documentazione del rifiuto, della restrizione o del differimento dell'informazione sia da conservare più a lungo rispetto ai verbali secondo l'articolo 3 AP-OLPD. Insieme ad altri chiedono un accorciamento.[417] Tuttavia, DigiGes sottolinea l'importanza di questa norma, affinché la persona interessata possa esercitare i propri diritti. Il disciplinamento è espressione del principio di trasparenza. Alcuni partecipanti sottolineano quindi che l'obbligo di conservazione andrebbe esteso a 5 anni.[418] Questo corrisponderebbe al termine di prescrizione per un gran numero di pretese legali.[419]

---

[409] Cantoni: LU; partiti: Alleanza del centro; organizzazioni: UPSA, Bär & Karrer, Creditreform, Datenschutzguide.ch, economiesuisse, EXPERTsuisse, H+, ASSOCIAZIONE DI COMMERCIO.swiss, IGEM, Migros, EPS, pharmasuisse, Ringier, ASP, FSA, ASB, Scienceindustries, usam, ASSL, BNS, SPA, UCS, SwissHoldings, suisa, swissICT, swissprivacy.law, swissstaffing, vsi, VSP, VUD, Walderwyss.

[410] Organizzazioni: Pharmasuisse, USI, ASB, UCS.

[411] Organizzazioni: UPSA, economiesuisse, Migros, Scienceindustries, ASSL, SwissHoldings.

[412] Cantoni: AR, AG, NW, SH, SZ, VD, ZH, organizzazioni: responsabile della protezione dei dati SZ/OW/NW; privatim, Ringier, SPA.

[413] Organizzazioni: H+, IGEM, BNS, swissICT, VUD.

[414] Cantoni: AG, AR, BL, GR, NW, OW, SH, SZ, VD, ZH, organizzazioni: responsabile della protezione dei dati SZ/OW/NW; H+, IGEM, privatim, Ringier, VUD.

[415] p. es. organizzazione: BNS.

[416] Organizzazioni: economiesuisse, Migros, Scienceindustries, SPA, Walderwyss.

[417] Organizzazioni: Bär & Karrer, curafutura, FER, FMH, EPS, proFonds, Ringier, ASP, ASA, SWICO, vsi, VSP.

[418] Organizzazioni: ASDPO, DFS, Swimag.

[419] Organizzazione: Swimag.

Più in dettaglio, si rileva che nel testo tedesco la terminologia relativa a «Informationen» e «Auskünfte» andrebbe unificata.[420]

3.2.21 Art. 21 AP-OLPD: Competenza

Economiesuisse suppone che entrambi i capoversi dell'articolo 1 riguardano il trattamento coordinato di una richiesta di informazioni presso più titolari. Tuttavia, questo non è espresso abbastanza chiaramente.[421] In questo senso, si critica anche il fatto che la norma non è formulata abbastanza chiaramente. Se il disciplinamento va oltre il coordinamento, le conseguenze giuridiche della «noncompetenza» non sono chiare.[422] Interpretando anch'essa la norma come una norma di coordinamento, ASDPO osserva che purtroppo non c'è una disposizione che regoli la questione generale delle responsabilità sulla base dell'articolo 26 RGPD.

Cpv. 1

Nel capoverso 1, diversi partecipanti chiedono di chiarire che si tratta di una responsabilità congiunta.[423] Per quanto riguarda le autorità federali, si osserva che l'obbligo di trasmettere la domanda è in ogni caso un principio di diritto amministrativo che nasce dalla relazione sovrana tra lo Stato e i cittadini.[424] Per quanto riguarda i privati, ci sono diverse critiche. Alcuni partecipanti ritengono che un obbligo per i privati di trasmettere la domanda sia sproporzionato, poiché in una relazione di diritto privato sono le parti a determinare autonomamente i loro diritti e obblighi. L'obbligo implicherebbe un onere per il titolare di diritto privato senza rafforzare i diritti delle persone interessate.[425] FRC, d'altra parte, accoglie con favore il fatto che la domanda di informazioni possa essere presentata a qualsiasi titolare del trattamento. Questo rafforzerebbe i diritti della persona interessata.

A ciò si aggiunge una critica generale al capoverso 1. Nella pratica, un titolare del trattamento non può sempre chiarire se e quali titolari sarebbero altrettanto competenti. Pertanto, il titolare spesso non può soddisfare la richiesta.[426] L'inoltro in casi poco chiari minerebbe la protezione dei dati.[427] La prima frase dovrebbe quindi specificare che si può trattare solo di dati per i quali diversi titolari del trattamento sono congiuntamente responsabili.[428] L'Alleanza del Centro sostiene anche che, in base alla formulazione attuale, un titolare del trattamento potrebbe rifiutare una possibile responsabilità a sua discrezione e inoltrare senza giustificazione la domanda di informazioni a un responsabile del trattamento.

ASB nota anche che potrebbero sorgere problemi nel caso di i titolari domiciliati all'estero. anche perché le domande di informazioni non dovrebbero essere trasmesse per mezzo di e-mail non protette.

[420] Organizzazioni: ASDPO, swissprivacy.law.

[421] Organizzazioni: economiesuisse, ASB.

[422] Organizzazioni: IGEM, santésuisse, suva, VUD.

[423] Organizzazioni: Bär & Karrer, DFS, IGEM, USI, ASB, suva, VUD.

[424] Cantoni: AG, AR, BS, GL, SH, SO, UR, VD, ZH; organizzazioni: privatim.

[425] Cantoni: AG, AR, BS, SH, SO, VD, ZH; organizzazioni: privatim.

[426] Partiti: Alleanza del centro; organizzazioni: economiesuisse, ASB.

[427] Organizzazioni: economiesuisse, ASB.

[428] Organizzazione: ASB.

Cpv. 2

ASB sostiene che il secondo capoverso non ha rilevanza, poiché il responsabile del trattamento rientra nel capoverso 1. Si tratta della gestione coordinata delle domande di informazioni.

Considerando il capoverso molto problematico, alcuni partecipanti ritengono che il passaggio dell'obbligo d'informazione dal titolare al responsabile del trattamento comprometta il disciplinamento della competenza secondo l'articolo 25 capoverso 4 nLPD e che il capoverso 2 vada quindi stralciato.[429] Si sostiene che è compito del titolare ottenere dal responsabile le informazioni necessarie per la fornitura di informazioni e decidere in merito alla domanda di informazioni.[430]

Inoltre, secondo il capoverso 2, il responsabile del trattamento ha la possibilità di non ritrasmettere la domanda di informazioni e non rispondervi, anche se in realtà dovrebbe essere in grado di farlo.[431] L'Alleanza del Centro critica anche il fatto che la formulazione permetterebbe a un titolare di negare la propria competenza per attribuirla ad un responsabile. SWICO osserva che per ragioni di conformità, un titolare non può permettersi di trasmettere semplicemente la domanda di informazioni invece di impostare i processi interni necessari.

economiesuisse suggerisce che sarebbe meglio obbligare il responsabile a sostenere il titolare nel fornire informazioni.[432] In pratica, i responsabili spesso non sono in grado di soddisfare tali domande o sono addirittura obbligati per contratto a non farlo.[433]

3.2.22 Articolo 22 AP-OLPD: Termine

Cpv. 1

Un gran numero di partecipanti commenta che il termine può iniziare a decorrere solo se la domanda è chiara e la persona interessata correttamente identificata.[434] La domanda deve inoltre essere presentata in modo formalmente corretto.[435] DigiGes al contrario sottolinea che il termine non dovrebbe sottostare ad alcuna condizione. Questo darebbe ai titolari troppo potere discrezionale, il che limiterebbe considerevolmente i diritti delle persone interessate. Il Cantone di Soletta vorrebbe che risultasse chiaro dalla disposizione che le informazioni, come richiesto dall'articolo 25 capoverso 7 nLPD, vanno fornite di norma entro 30 giorni.

Inoltre, alcuni desiderano che si tenga conto delle ferie giudiziarie, poiché sono caratterizzate da molte assenze.[436]

[429] Cantoni: SG; organizzazioni: HÄRTING Rechtsanwälte, USI, swissICT.

[430] Cantoni: GL, SG; organizzazioni: HÄRTING Rechtsanwälte, SWICO.

[431] Organizzazioni: economiesuisse, IGEM, santésuisse, ASB, suva, VUD.

[432] Anche l'organizzazione: SWICO.

[433] Organizzazioni: economiesuisse, ASB, VUD.

[434] Organizzazioni: UPSA, auto schweiz, economiesuisse, Creditreform, IGEM, EPS, Ringier, ASP, santésuisse, FSA, ASB, usam, ASSL, SPA, suva, Swiss Insights, swissprivacy.law, vsi, VSP, VUD, Walderwyss.

[435] Organizzazioni: Creditreform, EPS, ASP, usam, swissprivacy.law, vsi, VSP.

[436] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

Cpv. 2

Il Cantone di Soletta osserva che dal tenore della disposizione dovrebbe risultare più chiaro che i termini per rispondere alle domande di informazioni superiori a 30 giorni rappresentano un'eccezione. In questo senso, alcuni partecipanti vorrebbero aggiungere un termine massimo per limitare il margine di manovra dei titolari e rendere impossibile la proroga a tempo indeterminato del termine. Ciò proteggerebbe i diritti dell'interessato.[437]

ASDPO propone che il capoverso 2 includa anche la comunicazione di un rifiuto, una restrizione o un differimento dell'informazione.

Swimag propone che il termine per fornire informazioni sia ridotto a 3 giorni se la persona interessata acconsente allo scambio o alla comunicazione elettronica e presenta la richiesta di informazioni firmata con una firma elettronica certificata qualificata secondo la legge del 18 marzo 2016[438] sulla firma elettronica e l'articolo 14 CO oppure se presenta l'Id-e con una nota esplicita. Questo sarebbe conforme alla realtà moderna.

3.2.23 Art. 23 AP-OLPD: Eccezioni alla gratuità

Cpv. 1

Si chiede di chiarire almeno nel rapporto esplicativo l'espressione «onere sproporzionato». Questo è particolarmente importante perché imporre delle spese potrebbe minare il diritto all'informazione della persona interessata.[439]

SWICO suggerisce che anche le richieste di informazioni da parte di querulomani siano esplicitamente contemplate da questa disposizione.[440]

Cpv. 2

Diversi partecipanti sottolineano che la partecipazione alle spese dovrebbe essere l'eccezione e sostengono che l'informazione dovrebbe essere sempre gratuita.[441] La partecipazione alle spese non dovrebbe diventare un mezzo per i titolari del trattamento per impedire agli interessati di accedere ai loro dati. Pertanto, la partecipazione alle spese dovrebbe essere ammessa solo «in via eccezionale».[442] DigiGes fa notare che un'eccezione all'esenzione da spese esiste già oggi e viene spesso usata in modo abusivo per estendere le possibilità di respingere le richieste di accesso ai dati. Pertanto, questa eccezione alla gratuità dovrebbe essere eliminata del tutto. Anche altri partecipanti chiedono che la fornitura di informazioni sia sempre gratuita, indipendentemente dallo sforzo che comporta, poiché secondo il principio della «privacy by design» è responsabilità del titolare del trattamento gestire un sistema che permetta un facile accesso ai dati trattati. Se i titolari del trattamento dei dati dovessero fare uno sforzo «sproporzionato» nel caso di una richiesta di informazioni a causa del loro sistema inadeguato, le spese non dovrebbero essere a carico della persona interessata.[443] Il PS chiede almeno di non alzare il tetto delle spese.

La Fondazione per la protezione dei consumatori sostiene che la la partecipazione alle spese dovrebbe applicarsi solo alle richieste di informazioni oggettivamente querulomani. Altri partecipanti ritengono che anche queste andrebbero respinte senza addebitare spese, poiché

[437] Organizzazioni: DigiGes, FRC, I VERDI, Fondazione per la protezione dei consumatori, swissICT.

[438] FiEle; RS 943.03.

[439] Cantoni: GE, SG; Organisationen: ASSOCIAZIONE DI COMMERCIO.swiss, swissICT.

[440] Altrettanto l'organizzazione: ASA.

[441] Partiti: I VERDI, PS; organizzazioni: DigiGes, FRC, Fondazione per la protezione dei consumatori.

[442] Organizzazione: FRC.

[443] Partiti: I VERDI, PPS; organizzazioni: DigiGes, Swimag.

altrimenti la disposizione potrebbe essere interpretata in modo abusivo.[444] In modo analogo, il Cantone di Turgovia chiede di mantenere la disposizione originaria dell'articolo 2 capoverso 1 lettera a OLPD secondo cui la partecipazione alle spese può essere prevista se le informazioni richieste sono già state comunicate al richiedente nei 12 mesi prima dell'inoltro della domanda e non sussiste più un interesse degno di protezione.

Il PPS osserva che per quanto riguarda le eccezioni alla gratuità, si dovrebbe distinguere tra le imprese il cui il trattamento di dati è solo di natura amministrativa e le imprese il cui modello di business è basato sulla raccolta, analisi, fornitura e/o utilizzo dei dati.

FRC vorrebbe che il titolare del trattamento non solo quantifichi le spese straordinarie, ma spieghi anche le ragioni di tali spese.

In contrasto con le opinioni precedentemente descritte, molti partecipanti notano che il limite di 300 franchi della partecipazione alle spese è troppo basso e andrebbe alzato. Rispetto allo sforzo che comporta una domanda di informazioni, 300 franchi sono una cifra sproporzionatamente bassa.[445] santésuisse osserva che le domande generali di informazioni sui dati sono aumentate massicciamente negli ultimi anni. Inoltre, la quantità di dati richiesti è in aumento. Il Cantone di Soletta fa inoltre notare che le domande di informazioni potrebbero, in casi eccezionali, generare una notevole quantità di lavoro per i titolari. VUD sottolinea che l'importo dovrebbe avere un effetto deterrente, in modo che le persone interessate richiedano informazioni solo nei casi appropriati.[446]

Singolipartecipanti osservano che anche il RGPD non conosce alcun limite in termini di importo, ma richiede solo che quest'ultimo sia «ragionevole».[447] Il Cantone di Ginevra propone un'armonizzazione con l'iniziativa parlamentare sul disciplinamento degli emolumenti in merito al principio della trasparenza nell'ammistrazione[448] e quindi un tetto massimo delle spese pari a 2000 franchi.

Cpv. 3

Si chiede che la persona che richiede le informazioni sia tenuta ad acconsentire esplicitamente alla partecipazione alle spese. L'assenza di una risposta non deve essere interpretata come consenso.[449] Questo sarebbe vantaggioso per il titolare, poiché non dovrebbe fare sforzi eccessivi per garantire il pagamento.[450] Inoltre, garantirebbe la certezza del diritto per le persone interessate,[451] che dovrebbero pagare un massimo di 300 franchi.[452]. Il Cantone di Vaud osserva che questa disposizione potrebbe essere completata da un riferimento alle pertinenti disposizioni in materia di protezione dei dati, che disciplinano la procedura da seguire se la persona interessata contesta l'emolumento richiesto.

FER osserva alla luce della fornitura di informazioni entro 30 giorni, un termine di riflessione di 10 giorni è troppo lungo. Andrebbe quindi ridotto a 7 giorni. Altri partecipanti chiedono di specificare l'inizio del termine oppure di far decorrere il termine di risposta di 30 giorni solo dopo la scadenza del periodo di riflessione di dieci giorni o, eventualmente, dopo la conferma dell'accettazione delle spese, in modo che non sia di fatto ridotto a 20 giorni.[453]

---

444 Partiti: I VERDI; organizzazioni: DigiGes, Swimag: desiderano una definizione legale di querulomane.

445 Cantoni: SO (500 CHF), GE; partiti: Alleanza del centro, organizzazioni: UPSA, IS (1000 CHF), ASPS (1000 CHF), auto schweiz, Creditreform (1000 CHF), curafutura, CURAVIVA (1000 CHF), economiesuisse, Gastrosuisse, ASSOCIAZIONE DI COMMERCIO.swiss, HÄRTING Rechtsanwälte, IGEM (3000 CHF), INSOS (1000 CHF), EPS (1000 CHF), ASP (1000 CHF), santésuisse (2000 CHF), ASB, senesuisse (1000 CHF), usam (1000 CHF), ASSL (5000 CHF), SPA, Spitex (1000 CHF), suva (3000 CHF), ASA, swissstaffing (1000 CHF), vsi, VSP (1000 CHF), VUD (mindestens 3000 CHF), Walderwyss (5000 CHF).

446 Organizzazioni: IGEM, suva, VUD.

447 Organizzazioni: VUD, IGEM, suva.

448 Iniziativa parlamentare. Disciplinamento degli emolumenti. Principio della trasparenza nell'Amministrazione federale. Rapporto della Commissione delle istituzioni politiche del Consiglio nazionale (admin.ch).

449 Organizzazioni: ASDPO, FRC, santésuisse, Fondazione per la protezione dei consumatori, swissprivacy.law.

450 Organizzazioni: HTC, santésuisse, swissprivacy.law.

451 Organizzazione: Santésuisse.

452 Organizzazione: Fondazione per la protezione dei consumatori.

453 Organizzazioni: ASDPO, economiesuisse, HÄRTING Rechtsanwälte, HDC, IGEM, FSA, ASB, SPA, swissICT, swissprivacy.law, VUD.

3.2.24 Articolo 24 AP-OLPD: Diritto alla consegna o alla trasmissione dei dati (portabilità dei dati)

Per quanto riguarda l'articolo 24 AP-OLPD, si nota che la «portabilità dei dati» è stata introdotta solo durante il dibattito parlamentare sulla revisione della LPD. Di conseguenza, il messaggio sulla revisione della LPD non conteneva spiegazioni.[454] Non è quindi sufficiente, nell'ordinanza, fare riferimento esclusivamente agli articoli sul diritto d'informazione. Serve invece un disciplinamento dettagliato, la cui necessità non deve essere sottovalutata.[455] Alcuni partecipanti sottolineano che la portabilità dei dati è una conquista centrale del mondo digitale, che purtroppo è sempre più diviso in compartimenti di dati. I Verdi ritengono importante un regolamento preciso.[456]

Bär & Karrer afferma che l'interessato persegue un interesse diverso nell'esercizio del diritto alla consegna o alla trasmissione dei dati rispetto all'esercizio del suo diritto d'informazione. Gli effetti "lock-in" possono essere contrastati solo se gli interessati ricevono i dati in un formato strutturato, diffuso e leggibile elettronicamente. Di conseguenza, nel caso del diritto alla consegna e alla trasmissione, è cruciale che il titolare dei dati fornisca i dati in un determinato formato. Nel caso del diritto d'informazione, invece, questo è irrilevante.

Pertanto, andrebbero ad esempio specificamente regolamentati i «formati elettronici usuali». Sarebbe anche pertinente regolare l'«onere sproporzionato» nella trasmissione diretta da un titolare di dati a un altro. Inoltre, per quanto riguarda l'eccezione della gratuità, è concepibile una regolamentazione diversa da quella del diritto d'informazione, poiché non è prioritaria la protezione della personalità, bensì il valore economico dei dati.[457] SwissICT sostiene che se la disposizione restasse invariata, l'articolo 22 AP-OLPD (termine) non andrebbe applicato, per evitare contraddizioni. Swimag ritiene che l'articolo 20 dovrebbe essere pienamente applicabile, ma non l'articolo 23 AP-OLPD.

Alcuni partecipanti sottolineano che il diritto alla portabilità dei dati non può essere assoluto.[458] In nessun caso può portare all'obbligo di utilizzare sistemi di trattamento dei dati standardizzati.[459] Tale diritto dovrebbe sussistere solo se il trattamento dei dati personali può avvenire in formati diffusi.[460] Secondo usam, l'ordinanza andrebbe completata. Alcuni partecipanti chiedono di rinunciare all'obbligo di usare sistemi di trattamento dei dati tecnicamente compatibili.[461]

HDC sostiene fondamentalmente che a causa dell'adozione dell'articolo 28 nLPD dal RGPD, che ha una logica diversa, i dati che vengono trattati senza una violazione della personalità (e quindi senza consenso e contratto) ai sensi dell'articolo 30 nLPD non sono soggetti al diritto di consegna.

[454] Organizzazioni: UPSA, auto schweiz, usam, ASSL, SPA, Swiss Insights.

[455] Cantoni: AG, AR, SH, VD, ZH; organizzazioni: auto schweiz, I VERDI, privatim, usam, SPA, Swiss Insights.

[456] Partiti: I VERDI; organizzazioni: Bär & Karrer.

[457] Cantoni: AG, AR, SH, VD, ZH; organizzazioni: privatim.

[458] Organizzazioni: Creditreform, VSP, EPS, ASP, usam, vsi.

[459] Organizzazioni: ASSL, UPSA, Swiss Insights, auto schweiz.

[460] Organizzazioni: Creditreform, EPS, ASP, usam, vsi, VSP.

[461] Organizzazioni: UPSA, Auto schweiz (tutto nella formulazione concreta proposta), usam, ASSL, Swiss Insights.

3.2.25 Articolo 25 AP-OLPD: Consulente per la protezione dei dati

Cpv. 1

La proposta è esplicitamente accolta con favore da alcuni dei partecipanti.[462] Altri partecipanti sono invece critici. Secondo i Cantoni, l'articolo 25 AP-OLPD si basa poco all'articolo 10 capoverso 2 nLPD,[463] poiché è stato ripreso dall'ordinanza precedente.[464] L'articolo 10 capoverso 2 nLPD prevede ora tra i compiti dei consulenti per la protezione dei dati anche la formazione e la consulenza nonché la partecipazione all'applicazione delle norme sulla protezione dei dati. Pertanto, i compiti di cui all'articolo 25 AP-OLPD non sono i compiti da eseguire, ma solo la loro parziale concretizzazione. Questo andrebbe precisato nella norma.[465]

Alcuni Cantoni suggeriscono di aggiungere, ad esempio, l'espressione «in particolare».[466] Sorge anche la richiesta di lasciare solo l'articolo 10 capoverso 2 nLPD, che è formulato in modo più completo.[467] DFS raccomanda di specificare meglio i compiti dei consulenti per la protezione dei dati, fissati in modo troppo blando. Oltre alla partecipazione alla valutazione d'impatto della protezione dei dati, andrebbero elencati anche i compiti dei consulenti che servono alla promozione della protezione dei dati. Per esempio, i consulenti per la protezione dei dati dovrebbero essere più attivi nella prevenzione.[468] ASDPO suggerisce un inventario o una descrizione funzionale.

Si sostiene anche che sia concettualmente errato che i consulenti per la protezione dei dati debbano «rispettare» i compiti, dovrebbero invece «assumerli».[469]

SWICO sostiene che i compiti dovrebbero essere elencati come un dovere legale personale dei consulenti privati per la protezione dei dati, il che comporterebbe questioni di diritto della responsabilità senza un corrispondente chiarimento. Sono necessari chiarimenti o revisioni sui punti menzionati. Inoltre, altri partecipanti propongono di evitare una formulazione imperativa, poiché i consulenti per la protezione dei dati per i privati sono volontari. Se la disposizione dovesse essere intesa così che anche i privati fossero obbligati ad avere degli incaricati della protezione dei dati, non vi sarebbe alcuna base legale a sostegno.[470]

SPA osserva che la demarcazione tra i consulenti per la protezione dei dati e il titolare non è chiara se un'impresa ha già un consulente per la protezione dei dati ai sensi dell'articolo 37 RGPD.

Lett. a

Alcuni partecipanti sottolineano che l'articolo 10 capoverso 2 nLPD non contiene un mandato per regolare una verifica generale di tutti i trattamenti di dati personali, anche se la lettera a ora lo prevede.[471] L'obbligo di controllare tutti i trattamenti di dati contraddice anche l'approccio basato sui rischi di cui all'articolo 8 nLPD. L'implicazione nel rapporto esplicativo secondo cui ogni trattamento va controllato è errata. Si possono effettuare verifiche orientate al rischio.[472]

[462] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

[463] Cantoni: AI, AG, AR, GR, NW, SH, SZ, UR, VD, ZH; organizzazioni: responsabile della protezione dei dati SZ/OW/NW, privatim.

[464] Organizzazione: SWICO.

[465] Cantoni: AG, AR, GR, NW, SH, SZ, UR, VD, ZH; organizzazioni: Bär & Karrer, responsabile della protezione dei dati SZ/OW/NW, privatim, SPA. Bär & Karrer vorrebbe che si chiarisse se i compiti sono elencati in modo esaustivo.

[466] Cantoni: NW, OW, SZ.

[467] Cantoni: BS; organizzazioni: FSA.

[468] Organizzazioni: ASDPO, DFS.

[469] Organizzazioni: IGEM, ASB, suva VUD.

[470] Cantoni: LU; organizzazioni: ASDPO, SPA.

[471] Cantoni: BS, SG; organizzazioni: Curafutura, ASA.

[472] Cantoni: LU; organizzazioni: IGEM, ASA, suva, VUD.

Di conseguenza, non è chiaro in che misura le operazioni di trattamento debbano essere controllate (tutte, alcune, solo quelle presentate, solo secondo il rischio).[473] Economiesuisse afferma che esiste solo un obbligo di consultazione e che, al di fuori di questo, i consulenti per la protezione dei dati operano solo a titolo di consulenza generale. In questo senso, l'obbligo di controllo secondo il capoverso 1 lettera a andrebbe limitato al trattamento dei dati «loro sottoposti».[474] HÄRTING Rechtsanwälte, invece, sottolinea che, a differenza del RGPD, il legislatore ha dichiarato esplicitamente che i consulenti per la protezione dei dati devono anche garantire la protezione dei dati e possono e dovrebbero intervenire essi stessi anziché avere solo una funzione di garanti della conformità o di controllo. Secondo VUD, tuttavia, non è chiaro quali sarebbero le conseguenze se non si ottemperasse a questo compito di controllo generale.[475]

Anche il Cantone di Basilea Città lamenta che un tale obbligo di controllo generale è sproporzionato. L'obbligo di controllo non ha senso nella misura in cui trasforma i consulenti per la protezione dei dati in «poliziotti». Invece, la funzione consultiva dovrebbe essere sottolineata laddove le autorità responsabili intendano coinvolgere i consulenti.[476] Si afferma che da un punto di vista pratico, è impossibile controllare ogni trattamento di dati a causa dell'enorme numero di trattamenti coinvolti. I consulenti per la protezione dei dati non sarebbero nemmeno a conoscenza di ogni trattamento di dati degno di controllo.[477] Inoltre, si critica il fatto che la verifica supplementare del trattamento dei dati personali e la valutazione d'impatto della protezione dei dati porterebbe a un trasferimento di fatto della responsabilità ai consulenti per la protezione dei dati. L'ordinanza dovrebbe esplicitamente escludere questo scenario.[478]

In modo molto dettagliato, santésuisse nota che non ü necessario inserire il sintagma «nonché le relative condizioni», poiché l'esame dei prerequisiti fa parte del controllo.

Lett. b

Il capoverso 1 lettera b contraddice anche la funzione di consulenza descritta[479] e la libertà organizzativa dei titolari, che dovrebbero determinare gli obblighi in considerazione delle circostanze concrete all'interno dell'impresa.[480] Una tale invasione dell'autonomia privata avrebbe dovuto essere prevista a livello di legge.[481] D'altra parte, si sostiene anche che la sezione è superflua o ripetitiva a causa della deroga prevista dall'articolo 23 capoverso 4 nLPD.[482]

La norma contraddice anche numerosi regolamenti specifici di vari rami.[483] Inoltre, la disposizione viola il modello di difesa a tre linee stabilito come standard globale.[484]

IGEM sottolinea che la semplice presentazione di una valutazione d'impatto sulla protezione dei dati non è sufficiente. Piuttosto, i consulenti per la protezione dei dati devono partecipare alla preparazione della valutazione d'impatto. In tale contesto dovrebbere essere esaminate la valutazione dei rischi e le misure proposte.[485]

Alcuni partecipanti suggeriscono un'aggiunta che permetterebbe di «informare gli organi superiori [dei rispettivi enti privati o federali] nei casi più importanti».[486]

---

[473] Organizzazioni: Le banche domestiche, la Posta, economiesuisse, IGEM, ASB, suva, VUD.

[474] Anche le organizzazioni: La Posta, ASB, swissICT (implicito).

[475] Anche le organizzazioni: IGEM, suva.

[476] Organizzazioni: IGEM, suva, swissICT (sinngemäss), UBCS, VUD.

[477] Organizzazioni: La Posta, ASB, UBCS.

[478] Cantoni: SG; organizzazioni: curafutura

[479] Organizzazioni: La Posta, economiesuisse, ASB, swissICT (implicito), UBCS.

[480] Organizzazioni: La Posta, economiesuisse, ASB, ASA.

[481] Organizzazioni: La Posta, economiesuisse, ASB, swissICT (implicito).

[482] Organizzazioni: HÄRTING Rechtsanwälte, ASB.

[483] Organizzazioni: La Posta, ASB, swissICT (implicito), UBCS.

[484] Organizzazioni: econmiesuisse, ASB, swissICT (per analogia).

[485] Anche l'organizzazione: suva.

[486] Organizzazioni: economiesuisse, ASB, VUD.

Cpv. 2

Economiesuisse nota che la lettera b disciplina giustamente un diritto di intervento. Tuttavia, sarebbe auspicabile integrare questo diritto d'intervento secondo la lettera b con un diritto di ascesa in una nuova lettera c. Questo è necessario affinché i consulenti per la protezione dei dati, oltre a doversi fidare dei documenti messi a loro disposizione quando effettuano controlli interni alle imprese in merito al rispetto delle norme sulla protezione dei dati, possano anche imporre l'ottenimento di informazioni e documenti aggiuntivi.[487]

Questo creerebbe una serie di strumenti affinché in circostanze complesse o nel caso di violazioni particolarmente gravi degli obblighi di protezione dei dati i responsabili della protezione dei dati possano essere ascoltati a un livello gerarchico superiore e ottenere una decisione. In alternativa sarebbe possibile rivolgersi a un organo di controllo o agire per via gerarchica d'intesa con detto organo. Senza una tale norma, i consulenti per la protezione dei dati si esporrebbero al rischio di dover rispondere essi stessi delle violazioni.[488] ASDPO ritiene, tuttavia, che nell'articolo 25 AP-OLPD andrebbe chiarite comunque le responsabilità civili o penali dei consulenti per la protezione dei dati.

santésuisse constata che non esiste una norma per i consulenti privati in materia di protezione dei dati analoga all'articolo 28 AP-OLPD, che specifichi l'indipendenza dei consulenti il loro essere vincolati alle direttive.

3.2.26 Articolo 26 AP-OLPD: Eccezione all'obbligo di tenere un registro delle attività di trattamento

In generale la deroga è accolta con favore[489]. Il limite di 250 collaboratori è basato sulla legge della società per azioni.[490] CP ritiene che la grande maggioranza delle PMI beneficerebbe di questa eccezione. Questo è in linea con l'approccio basato sui rischi della nLPD. Il settore privato vorrebbe persino vedere un ulteriore allentamento o chiarimento delle disposizioni, affinché le piccole imprese siano meno oberate. Spitex Svizzera scrive che l'eccezione prevista non si applicha a molte imprese che trattano dati personali particolarmente sensibili su larga scala o fanno parte di un gruppo che impiega più di 250 collaboratori in totale.[491] Alcuni partecipanti preferirebbero che il criterio fosse una media di 250 posti a tempo pieno all'anno anziché solo 250 collaboratori.[492]

Tuttavia, molti partecipanti criticano che i requisiti del trattamento molto esteso di dati personali degni di particolare protezione o di una profilazione con un rischio elevato non coprirebbero tutti i trattamenti di dati critici per i diritti personali. Anche in questo caso dovrebbere essere ripresi, come nell'articolo 4 capoverso 1 AP-OLPD, i requisiti della valutazione d'impatto sulla protezione dei dati.[493] Anche FRC osserva che pur essendo lodevole limitare l'eccezione. le restrizioni corrono il rischio di essere compromesse se non si definiscono meglio i concetti di il «vasta scala» e la «profilazione ad alto rischio». Ci si chiede anche se il trattamento di dati personali degni di particolare protezione non debba costituire di per sé un'eccezione, anche

[487] Anche l'organizzazione: ASB.

[488] Organizzazioni: economiesuisse, ASB.

[489] Cantoni: LU; organizzazioni: IS, ASPS, CP, CURAVIVA, HDC, INSOS, proFonds, senesuisse, Spitex Svizzera, SwissFoundations.

[490] p. es. nel caso di eccezioni alla revisione ordinaria secondo l'articolo 727, capoverso 2 CO.

[491] Anche le organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse.

[492] Organizzazioni: ProFonds (se la media annuale di 250 posti a tempo pieno viene superata in due esercizi consecutivi, le fondazioni e le associazioni devono effettuare una revisione ordinaria ai sensi dell'articolo 727 CO), FSA, swissICT, VUD.

[493] Cantoni: AG, AR, GR, NW, SH, SO, SZ, VD, ZH; partiti: I VERDI; organizzazioni: ASDPO, responsabile della protezione dei dati SZ/OW/NW, privatim.

nel caso in cui i dati personali non vengano trattati in modo particolarmente esteso. ASDPO vorrebbe che l'articolo fosse più fondato sull'articolo 30 capoverso 5 RGPD.

Alcuni si rammaricano anche del fatto che ci sia un'eccezione per le imprese con meno di 250 collaboratori.[494] Questo rende fin troppo facile minare lo strumento del registro delle attività di trattamento.[495] Tenere un registro è infatti un mezzo semplice per garantire che il titolare rispetti i suoi obblighi in materia di protezione dei dati.[496] È anche un esercizio essenziale di buongoverno per quanto riguarda la protezione e la sicurezza dei dati.[497] Inoltre, con gli strumenti di oggi, la creazione di un registro delle attività di trattamento non rappresenta più uno sforzo aggiuntivo significativo, nemmeno per le imprese individuali. D'altronde l'elenco serve alla sensibilizzazione e all'autoprotezione.[498] È particolarmente importante per le PMI, poiché elaborano volumi sempre maggiori di dati personali e sono quindi uno degli obiettivi prescelti degli attacchi da parte di hacker.[499]

ASB afferma che il tenore dell'articolo implica che il registro vada tenuto per tutte le attività di trattamento, a meno che non ci siano le condizioni per un'eccezione. Altri auspicano che venga chiarito se questa era l'intenzione.[500] Altri ancora suppongono che non possa essere inteso in questo modo o sostengono che l'obbligo di tenere un registro andrebbe limitato ai trattamenti che soddisfano i requisiti.[501] In questo modo, sia la protezione delle persone interessate sia le esigenze delle PMI possono essere adeguatamente prese in considerazione.[502] EXPERTsuisse vorrebbe anche che venissero chiarite le conseguenze in caso di tenuta dell'elenco dei trattamenti non conforme alle regole.

Diversi partecipanti sostengono che l'articolo 12 capoverso 5 nLPD permette un'eccezione all'obbligo di tenere un registro di trattamento solo se c'è un «rischio esiguo». Pertanto, si deve presumere che se né la lettera a né la lettera b sono soddisfatte, sussiste un rischio esiguo.[503] Questo limita fortemente il campo di applicazione della valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 22 nLPD.[504] Altri partecipanti ritengono che non è chiaro se solo questi due casi comporterebbero un rischio elevato e chiedono di chiarire se questo elenco sia esaustivo.[505] Inoltre, occorrerebbe chiarire se questo è anche il parametro per l'esecuzione di una valutazione d'impatto sulla protezione dei dati e se è possibile applicarlo anche all'obbligo di notifica secondo l'articolo 24 nLPD.[506] Si è anche notato che non è stata prevista l'eccezione per l'articolo 12 cpoversi 3 e 4 nLPD, bensì soltanto per il capoverso 5, il che porterebbe a risultati assurdi.[507]

---

[494] Organizzazioni: FRC, ASDPO.

[495] Come esempio, viene menzionata la formazione di una filiale, che poi assume esclusivamente il trattamento di dati personali particolarmente sensibili o la profilazione.

[496] Organizzazioni: FRC, ASDPO.

[497] Organizzazione: ASDPO.

[498] Organizzazione: Swimag.

[499] Organizzazione: FRC.

[500] Organizzazioni: EXPERTsuisse, USI, SWICO.

[501] Partiti: Alleanza del centro; organizzazioni: UPSA, auto schweiz, economiesuisse, HDC, IGEM, santésuisse, SAV, ASB, Scienceindustries, usam, ASSL, suva, Swiss Insights, VUD.

[502] Organizzazioni: UPSA, auto schweiz, economiesuisse, ASSL, Swiss Insights.

[503] Organizzazioni: UPSA, auto schweiz, economiesuisse, IGEM, ASB, ASSL, suva, Swiss Insights, VUD.

[504] Organizzazioni: IGEM, ASB, suva, VUD.

[505] Organizzazioni: Bär & Karrer, SWICO.

[506] Altrimenti non c'è un rischio elevato per le persone interessate. Organizzazioni: Bär & Karrer, SWICO.

[507] Organizzazioni: IGEM, ASB, suva, VUD.

Le FFS chiedono che, come sinora, grazie alla nomina di consulenti per la protezione dei dati le imprese di trasporto siano esentate dall'obbligo di notifica dei registri all'IFPDT secondo l'articolo 12 capoverso 4 nLPD.

Lett. a

In particolare, il trattamento di dati degni di particolare protezione «su vasta scala» non è considerata una concretizzazione abbastanza precisa e lascia troppo spazio all'interpretazione. L'espressione «vasta scala» dovrebbe quindi essere precisata.[508] FRC sottolinea anche che le nozioni vanno precisate per non compromettere la disposizione.

Come esempio di una definizione più precisa, l'economia menziona un limite di almeno 1000 record di dati.[509] SFF è più in generale a favore di una definizione stretta, che, per esempio, si riferisca al rapporto tra tutti i dati personali e i dati personali degni di particolare protezione. PS e USS, d'altra parte, sottolineano che l'espressione «trattamento su vasta scala» non dovrebbe essere interpretato in modo troppo restrittivo.

Lett. b

Il Cantone di Lucerna vorrebbe aggiungere «per la personalità o i diritti fondamentali della persona interessata» come requisito della profilazione ad alto rischio. Questo creerebbe chiarezza.

Più in generale, bisognerebbe prevedere dei periodi di transizione per i registri, dato che comporterebbero una grande mole di lavoro.[510] Inoltre, andrebbe specificato che i registri possono essere tenuti non solo per scritto, ma anche in un'altra forma che permetta la prova per testo.[511]

3.2.27 Articolo 27 AP-OLPD: Nomina

Si critica che sarebbe sproporzionato e impossibile da attuare nella pratica se ogni organo federale dovesse nominare i propri consulenti per la protezione dei dati.[512] Inoltre, secondo UTP, non esiste una base legale per l'obbligo di nominare consulenti per la protezione dei dati. Il Cantone di Svitto osserva che il diritto di protezione dei dati di Schengen richiede solo l'uso di consulenti per la protezione dei dati nei settori della polizia, del perseguimento penale e dell'esecuzione delle pene. Si osserva anche che l'articolo 23 OLPD prevede attualmente dei consulenti per la Cancelleria federale e ciascuno dei sette dipartimenti. Tuttavia, gli uffici federali sono molti di più. L'attuale formulazione andrebbe quindi mantenuta.[513]

Al contrario, PS esige che ogni organo federale nomini il proprio consulente per la protezione dei dati. Da un lato, questo è dovuto al fatto che ogni organo federale è abbastanza grande in termini di numero di collaboratori e di volume di dati trattati da giustificare un proprio consulente per la protezione dei dati. Dall'altro lato, si spiega con il fatto che i consulenti interni per la protezione dei dati conoscono meglio i collaboratori e la cultura operativa dell'organo federale interessato e potrebbero quindi svolgere i loro compiti in modo più efficace. Anche UTP è del parere che i consulenti per la protezione dei dati debbano conoscere i processi della rispettiva impresa per poter svolgere i loro compiti in modo professionale, e che la presenza di un solo consulente per la protezione dei dati per diversi organi federali è quindi poco sensata.

[508] Organizzazioni: IS, ASPS, CURAVIVA, EXPERTsuisse, FMH, ASSOCIAZIONE DI COMMERCIO.swiss, IGEM, INSOS, senesuisse, UPSC, usam, Spitex Svizzera, SSO, suva, VUD.

[509] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

[510] Organizzazioni: IGEM, santésuisse, FSA, ASB, VUD.

[511] Organizzazioni: UPSA, auto schweiz, economiesuisse, usam, ASSL, Swiss Insights.

[512] Cantoni: SZ; organizzazioni: CP, FER, UTP.

[513] Organizzazioni: CP, FER.

ASA rifiuta del tutto la nomina di consulenti per la protezione dei dati per gli organi federali. Ritiene che anche questo dovrebbe essere volontario e che si dovrebbe creare un incentivo corrispondente per la nomina. ASIP auspica un'esenzione dall'obbligo di nominare consulenti per la protezione dei dati per gli istituti di previdenza registrati secondo l'ordinanza del 10 e 22 giugno 2011 concernente la vigilanza nella previdenza professionale.

Il Cantone di Friburgo critica che la disposizione dovrebbe specificare come garantire l'indipendenza dei consulenti per la protezione dei dati e le sanzioni previste in caso di mancata indipendenza. Inoltre, ritiene che vada chiarito che la relazione tra i responsabili della protezione dei dati e i responsabili della sicurezza delle informazioni. Eventualmente si potrebbe anche prevedere che questi compiti siano assegnati ad una sola persona.

3.2.28 Articolo 28 AP-OLPD: Requisiti e compiti

Titolo

HÄRTING Rechtsanwälte critica il titolo della disposizione. Questo andrebbe specificato per chiarire che la norma si applica esclusivamente agli organi federali.

Cpv. 2

Lett. a

SwissICT chiede di stralciare il capoverso 2 lettera a, poiché un obbligo generale di verifica sarebbe troppo ampio. I consulenti per la protezione dei dati potrebbero fungere solo da interlocutori.[514] Classtime auspica l'introduzione di «classi di sensibilità dei dati», poiché la verifica del trattamento di dati personali deve essere svolta nel contesto dei casi d'applicazione e dei benefici del trattamento nonché della sensibilità.

I Cantoni e privatim criticano il fatto che non viene menzionato il compito di collaborazione all'applicazione delle norme sui dati, come previsto dall'articolo 10 capoverso 2, bensì solo la formazione e la consulenza. Si chiede un complemento.[515]

3.2.29 Articolo 29 AP-OLPD: Obblighi dell'organo federale

Cpv. 1

Il Cantone di Svitto osserva che i consulenti per la protezione dei dati non svolgono una funzione esterne all'organo di controllo della protezione dei dati, bensì specialisti interni e interlocutori per l'organo di controllo e l'ente pubblico responsabile. Pertanto, l'introduzione di diritti di consultazione globali non è da sostenere. Nello stesso senso, swissICT osserva che l'accesso è necessariamente legato ai compiti dei consulenti per la protezione dei dati e che la formulazione proposta è quindi troppo ampia.

Cpv. 2

Alcuni pochi partecipanti chiedono di precisare la disposizione nel senso che la pubblicazione di un indirizzo e-mail indicante la funzione dovrebbe essere sufficiente. Ciò permetterebbe di proteggere la personalità dei consulenti per la protezione dei dati.[516]

[514] Cfr. commenti all'articolo 25 AP-OLPD.

[515] Cantoni: AG, TG, SH, VD; organizzazioni: privatim.

[516] Organizzazioni: BNS, analogamente anche ASA, Walderwyss.

3.2.30 Articolo 30 AP-OLPD: Servizio di contatto dell'IFPDT

Santésuisse osserva che sarà difficile interagire con l'IFPDT a causa della drastica riduzione delle competenze dei consulenti aziendali per la protezione dei dati. L'indipendenza attuale viene limitata dall'attività di consulenza dei consulenti per la protezione dei dati.

3.2.31 Articolo 31 AP-OLPD: Informazione del consulente per la protezione dei dati

Si osserva che per questa disposizione dell'ordinanza non c'è una base legale sufficiente. Gli obblighi d'informazione e di notifica contenuti dovrebbero essere regolati a livello di legge.[517] SwissICT osserva che il trattamento automatizzato dei dati personali è oggi usuale. Un tale obbligo di autorizzazione generale per i progetti non può quindi essere voluto dal legislatore. In tal senso, l'articolo 35 capoverso 1 nLPD prevede l'obbligo di autorizzazione solo per il trattamento automatizzato di dati personali degni di particolare protezione. Ciò dovrebbe essere aggiunto nel progetto di ordinanza.[518]

ASA rifiuta l'obbligo per gli organi federali di informare i loro consulenti in materia di protezione dei dati nel caso di progetti di trattamento automatizzato dei dati. Quest'obbligo non costituisce alcun valore aggiunto per gli interessati e comporta un inutile onere amministrativo. La disposizione va quindi stralciata.

SFF critica il fatto che, rispetto OLPD vigente, l'«annuncio senza indugio» è stato sostituito con «informa tempestivamente». Poiché il termine «tempestività» è interpretabile, si crea un margine di interpretazione che mette in pericolo la certezza del diritto e l'applicazione uniforme della legislazione. Si potrebbero così legittimare eventuali ritardi nella trasmissione delle informazoni. Il termine originale «senza indugio» va quindi ripristinato.

Altri, invece, vogliono che il successivo «immediatamente» sia sostituito da «tempestivamente». Non è chiaro cosa dovrebbe significare «immediatamente». Inoltre, deve essere sufficiente che i requisiti della protezione dei dati siano presi in considerazione tempestivamente nel progetto.[519] BNS vorrebbe sostituire «immediatamente» con «in modo adeguato» o, come soluzione ottimale, eliminare del tutto l'espressione. Secondo curafutura, anche l'espressione «dopo la conclusione del progetto» non è chiara.

Le FFS ritengono che la disposizione contenga requisiti relativi a meri processi interni e quindi interferisca in modo sproporzionato con la libertà organizzativa delle imprese di trasporto. Le «imprese» responsabili dovrebbero essere libere di decidere come meglio implementare i propri metodi di processo. Non tutte le «imprese» usano il metodo HERMES per gestire i progetti. Secondo swissICT, la disposizione non può applicarsi a organi federali esterni come le casse pensione, in quanto in alcuni casi essi sono soggetti a speciali obblighi di segretezza.

3.2.32 Articolo 32 AP-OLPD: Notifica all'IFPDT

Alcuni partecipanti chiedono di stralciare l'articolo.[520] Esso non ha alcuna base legale.[521] Secondo il commento del messaggio sull'articolo 12 capoverso 4 nLPD, non dovrebbero risultare

[517] Organizzazioni: Curafutura, ASA.

[518] Anche l'organizzazione: HÄRTING Rechtsanwälte.

[519] Organizzazioni: DFS, IGEM, suva, VUD.

[520] Organizzazioni: Curafutura, IGEM, BNS, suva, SWICO, swissICT, VUD.

[521] Organizzazioni: Curafutura, DFS, IGEM, santésuisse, BNS, suva, ASA, SWICO, swissICT, VUD, Walderwyss.

modifiche rispetto al diritto vigente e attualmente non sussite alcun obbligo di notificare all'IFPDT le raccolte di dati previste.[522]

Si critica anche il fatto che le attività di trattamento automatizzato già pianificate devoo essere segnalate.[523] La notifica va effettuata al momento dell'approvazione del progetto o della decisione di sviluppare il progetto.[524] È quindi molto dubbio che sia rispettato il principio di proporzionalità dell'articolo 32 capoverso 1.[525] La disposizione implica un notevole sforzo (burocratico) aggiuntivo per la documentazione[526] poiché le decisioni concrete sono di solito prese solo nel corso di un progetto. Pertanto, le indicazioni richieste spesso non sono ancora disponibili al momento dell'informazione o non sono sufficientemente dettagliate.[527] Le FFS fanno notare che la disposizione non è praticabile per i suoi progetti, che non sono più pianificati nel classico «modello a cascata». Oggi la sua pianificazione avviene in modo agile e continuo. I termini usati nella disposizione sono quindi obsoleti. Si osserva anche che resta poco chiaro il momento a partire dal quale un processo è «pianificato».[528]

Il lavoro supplementare per una segnalazione così precoce non è giustificato, soprattutto perché, secondo il rapporto esplicativo, piuttosto che alla protezione della personalità serve alla pianificazione delle risorse dell'IFPDT.[529] Walderwyss è dell'opinione che l'IFPDT non può utilizzare queste informazioni poiché non ha le risorse per farlo.

È inoltre problematica la segnalazione di ogni operazione di trattamento automatizzato, non solo di quelle che presentano un (potenziale) rischio elevato.[530] Le FFS ritengono che l'obbligo di notificare all'IFPDT ogni singola operazione di trattemtno non manuale generi una mole di lavoro sproporzionata e non sia quindi opportuno. Inoltre, contraddice l'approccio basato sui rischi della nLPD. Altri partecipanti sottolineano inoltre che, pur essendo una disposizione transitoria per le attività di trattamento automatizzato, l'articolo 47 AP-OLPD non rappresenta uno sgravio in quanto, per i trattamenti già operativi, deve essere creato un registro e inviata una notifica all'IFPDT.[531]

Le FFS constatano che, secondo il diritto vigente, le imprese di trasporto non hanno l'obbligo di notificare all'IFPDT le raccolte di dati previste. Le imprese di trasporto che hanno consulenti per la protezione dei dati dovrebbero tuttora essere esentate dall'obbligo di notifica all'IFPDT.

3.2.33 Articolo 33 AP-OLPD: Carattere imprescindibile della fase sperimentale

Il Cantone di Vaud osserva che dovrebbe sussistere anche l'obbligo di consultare le autorità cantonali qualora esse siano interessate dai progetti.
SwissICT sostiene che un obbligo di autorizzazione dovrebbe essere previsto solo se il trattamento ha un forte impatto su dati personali degni di particolare protezione. Inoltre, la lettera c andrebbe stralciata, poiché è solo una possibile costellazione che deve essere esaminata. Allo

[522] Organizzazioni: IGEM, BNS, suva, VUD.

[523] Organizzazioni: Curafutura, DFS, IGEM, BNS, suva, SWICO, swissICT, VUD.

[524] Organizzazioni: IGEM, santésuisse, FFS, BNS, suva, SWICO, swissICT, VUD, Walderwyss.

[525] Organizzazioni: BNS, Walderwyss.

[526] Organizzazioni: Curafutura, DFS, IGEM, BNS, suva, SWICO, swissICT, VUD.

[527] Organizzazioni: IGEM, santésuisse, FFS, BNS, suva, SWICO, swissICT, VUD, Walderwyss.

[528] Organizzazioni: BNS, Walderwyss.

[529] Organizzazioni: Curafutura, DFS, IGEM, santésuisse, FFS, suva, ASA, VUD.

[530] Organizzazioni: Santésuisse, BNS, SWICO.

[531] Organizzazioni: IGEM, santésuisse, suva, VUD.

stesso modo, HÄRTING Rechtsanwälte vorrebbe che la fase sperimentale, in quanto test pilota, sia necessaria soltanto se è connessa ad un aumento del rischio per la persona interessata.

3.2.34 Articolo 34 AP-OLPD: Autorizzazione

SwissICT osserva che non sono specificate le conseguenze in caso di mancato rispetto della nLPD, o in quali casi l'autorizzazione possa essere revocata. In particolare, andrebbe specificata la pertinente procedura e le relative scadenze.

Cpv. 2

Santésuisse accoglierebbe con favore se, per la sicurezza della pianificazione, venisse definito un termine entro il quale ci si può aspettare un parere dell'IFPDT.

Inoltre, swissICT vorrebbe che il capoverso 2 lettera d parlasse di provvedimenti tecnici e organizzativi anziché di provvedimenti di sicurezza e di protezione dei dati. Inoltre, il capoverso 2 lettera e andrebbe stralciato, poiché un progetto di ordinanza non è necessario in ogni costellazione.

Cpv. 5

SwissICT è del parere che non è chiaro, per quanto riguarda il capoverso 5, se una proposta all'attenzione del Consiglio federale sia necessaria in ogni caso.

3.2.35 Articolo 35 AP-OLPD: Rapporto di valutazione

SwissICT chiede di stabilire che il rapporto deve essere consultato per ulteriori passi.

3.2.36 Articolo 36 AP-OLPD: Trattamento di dati per scopi impersonali

Si osserva che la disposizione è superflua, poiché la precisazione nell'articolo 36 AP-OLPD risulta già dall'articolo 39 nLPD.[532] ASA aggiunge che la disposizione nell'ordinanza causerebbe pertanto solo confusione e creerebbe incertezza giuridica.

SwissICT osserva che l'articolo 39 nLPD si applica solo al trattamento dei dati per scopi non personali da parte di organi federali che conducono ricerche, pianificazioni o statistiche. Tali organi federali non dovrebbero essere tenuti a verificare se il trattamento per la ricerca, la pianificazione o la statistica possa ancora avere una componente personale.

3.2.37 Articolo 39 AP-OLPD: Comunicazione di direttive e decisioni

UPSC osserva che sarebbe opportuno definire nell'ordinanza stessa il momento in cui l'IFPDT è coinvolto nei progetti di atti normativi relativi al trattamento dei dati personali, alla protezione dei dati e all'accesso ai documenti ufficiali. Questo creerebbe certezza giuridica ed eviterebbe di lasciare troppo spazio all'interpretazione.

DFS chiede perché l'amministrazione federale debba comunicare le proprie direttive all'IFPDT in forma anonimizzata. Le direttive relative alla legge sulla protezione dei dati sono condizioni quadro che si rivolgono a diversi destinatari e dovrebbero quindi, di norma, sottostare al principio della trasparenza.

3.2.38 Articolo 41 AP-OLPD: Autocontrollo

Santésuisse suggerisce che anche l'IFPDT sia obbligato a tenere un registro delle attività di trattamento. Non è chiaro perché esentarlo da tale obbligo.[533]

[532] Cantoni: AG, AI, GR, NW, SH, SZ, VD, ZH; organizzazioni: responsabile della protezione dei dati SZ/OW/NW, privatim, ASA, swissICT.

[533] Anche l'organizzazione: HÄRTING Rechtsanwälte.

Classtime è del parere che l'autocontrollo, che avverrebbe nel quadro di un'organizzazione di autoregolamentazione, andrebbe imposto, oltre che all'IFPDT, anche ai privati e alle autorità federali.

3.2.39 Articolo 42 AP-OLPD: Cooperazione con il Centro nazionale per la cibersicurezza (NCSC)

HDC critica, nel testo francese, il fatto che il capoverso 1 si riferisca alla «personne responsable de l'annonce», che è simile al termine «personne tenue d'annoncer» nell'articolo 24 capoverso 6 nLPD. Ritiene che sarebbe meglio usare il termine «titolare del trattamento».[534]

3.2.40 Articolo 43 AP-OLPD: Registro delle attività di trattamento degli organi federali

Le FFS rimandano all'articolo 27 AP-OLPD e desiderano nuovamente che le imprese di trasporto siano esentate dall'obbligo di annunciare i registri delle attività di trattamento presso l'IFPDT conformemente all'articolo 12 capoverso 4 nLPD, come è avvenuto finora in caso di nomina di consulenti per la protezione dei dati. Inoltre, un registro di tutte le attività di trattamento si qualifica come segreto commerciale e non può essere reso accessibile al pubblico senza restrizioni.

Curafutura osserva che l'articolo 43 AP-OLPD andrebbe adattato di conseguenza se l'articolo 32 AP-OLPD fosse stralciato.[535]

3.2.41 Articolo 44 AP-OLPD: Codice di condotta

FER si rammarica che il parere dell'IFPDT non sia ritenuto una decisione in senso formale (decisione impugnabile). D'altra parte, dal momento che si richiede un emolumento, vorrebbe che si fissasse un termine non troppo lungo per la consegna del parere. A tale proposito, considera appropriato un termine massimo di 30 giorni.

3.2.42 Articolo 45 AP-OLPD: Emolumenti

In generale

La critica fondamentale è che la disposizione inciterebbe praticamente le organizzazioni a violare la legge sulla protezione dei dati, poiché il sostegno dell'IFPDT non è finanziabile.[536] Pertanto, il disciplinamento degli emolumenti dovrebbe essere completamente riconsiderato e ragionevolmente.[537] Santésuisse chiede di rinunciare a un emolumento. Alcuni partecipanti sottolineano che la soglia di accesso all'IFPDT dovrebbe essere mantenuta bassa, soprattutto per la verifica dell'adeguatezza del codice di condotta (art. 59 cpv. 1 lett. a nLPD) o l'approvazione di clausole tipo di protezione dei dati (art. 59 cpv. 1 lett. b nLPD).[538]

Cpv. 1

[534] Anche l'organizzazione Swissprivacy.law.

[535] Anche l'organizzazione ASA.

[536] Organizzazioni: IS, ASPS, Creditreform, CURAVIVA, INSOS, EPS, ASP, santésuisse, senesuisse, usam, Spitex Svizzera, vsi, VSP.

[537] Organizzazioni: IS, ASPS, Creditreform, CURAVIVA, INSOS, EPS, ASP, senesuisse, usam, Spitex Svizzera, vsi, VSP.

[538] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

Si afferma che gli emolumenti non andrebbero calcolati in funzione del tempo impiegato, poiché le aziende non hanno alcuna influenza sulla complessità del problema o sull'efficienza dell'IFPDT.[539] Vanno fissati degli emolumenti massimi.[540]

Cpv. 2

Le tariffe orarie da 150 a 350 franchi sono troppo alte e fungerebbero addirittura de deterrente.[541] In particolare, si critica la discrepanza tra gli emolumenti dell'IFPDT e la partecipazione ai costi da parte degli individui per le richieste di informazioni.[542] Le attività dell'IFPDT sono nell'interesse della società e del pubblico. Non vi è alcuna ragione per cui le organizzazioni che hanno bisogno di servizi per operare in modo conforme alla protezione dei dati debbano sostenere costi così elevati. Ciò è contrario all'idea di servizio pubblico.[543] Spitex Svizzera commenta che deve essere fatta un'eccezione, soprattutto per il settore delle aziende sanitarie, che preveda tariffe orarie ragionevoli.[544]

SPA chiede che l'IFPDT comunichi in anticipo gli emolumenti previsti.

3.2.43 Articolo 47 AP-OLPD: Disposizione transitoria concernente la notifica all'IFPDT delle previste di trattamento automatizzato

Si osserva che se l'articolo 32 AP-OLPD venisse stralciato, andrebbe stralciato anche l'articolo 47 AP-OLPD.[545]

3.2.44 Articolo 48 AP-OLPD: Entrata in vigore

Alcuni partecipanti criticano il fatto che non ci siano periodi transitori nella nuova LPD, o che siano solo selettivi e incompleti.[546] Pertanto, il nuovo diritto deve essere già pienamente implementato al momento della sua entrata in vigore.[547] Tuttavia, la versione finale dell'ordinanza rivista non sarà disponibile e accessibile al pubblico prima della fine del 2021. Il DFGP prevede attualmente di far entrare in vigore la nuova legge nella seconda metà del 2022.[548]

Per una corretta attuazione del nuovo diritto bisogna tuttavia attendere la versione finale dell'ordinanza.[549] Solo allora potrà iniziare l'adattamento dei processi e l'implementazione e lo sviluppo di soluzioni supportate dalla tecnologia informatica. Prima dell'entrata in funzione di questi sistemi andrebbero effettuati dei test. Inoltre, i collaboratori dovrebbero essere formati in base alle loro rispettive funzioni.[550]

Da quanto detto sopra, risulta che il termine di attuazione di 6 mesi è estremamente breve. Secondo santésuisse, questo non è fattibile per la maggior parte delle imprese in quanto, come sostenuto da alcuni, il nuovo pacchetto legislativo è estremamente complesso e richiede molti

[539] Organizzazioni: IS, ASPS, Creditreform, CURAVIVA, GastroSuisse, INSOS, EPS, ASP, senesuisse, usam, Spitex Svizzera, vsi, VSP.

[540] Organizzazioni: CP, Creditreform, FER, EPS, ASP, vsi, VSP.

[541] Organizzazioni: IS, ASPS, Creditreform, CURAVIVA, INSOS, EPS, ASP, senesuisse, usam, Spitex Svizzera, vsi, VSP.

[542] Organizzazioni: Creditreform, EPS, ASP, usam, vsi, VSP.

[543] Organizzazioni: Creditreform, GastroSuisse, EPS, ASP, vsi, VSP.

[544] Organizzazioni: IS, ASPS, CURAVIVA, INSOS, senesuisse, Spitex Svizzera.

[545] Organizzazioni: Curafutura, ASA.

[546] Organizzazioni: Economiesuisse, santésuisse, ASB, ASA.

[547] Organizzazioni: Santésuisse, ASA.

[548] Organizzazione: Santésuisse.

[549] Organizzazioni: Economiesuisse, santésuisse, ASB, ASA.

[550] Organizzazioni: economiesuisse, ASB, ASA.

adeguamenti.[551] Al fine di perseguire un approccio il più globale possibile nell'implementazione, è necessario molto più tempo per l'attuazione.[552] ASB ed economiesuisse sono dell'opinione che un periodo di circa 2 anni sia necessario per le suddette attività. ASA ritiene adeguato un periodo di 1 anno.

Nell'UE, sono stati previsti 2 anni per l'attuazione dell RGPD. In Svizzera, invece, il Parlamento ha preso una decisione di base diversa per la nLPD. Le disposizioni transitorie, tuttavia, sono regolarmente trascurate nel processo parlamentare. Inoltre, le disposizioni transitorie andrebbero determinate secondo criteri esclusivamente oggettivi. Pertanto, è diventata prassi comune fissare, se necessario, nelle ordinanze le disposizioni transitorie supplementari. Naturalmente, un rinvio al 1° luglio 2023 per l'entrata in vigore dell'intero pacchetto legislativo rappresenterebbe un'opzione alternativa.[553]

Si propone quindi che l'entrata in vigore sia fissata non prima del 1° gennaio 2023.[554] Si propone inoltre che questo regime transitorio, considerato incompleto, vada completato a livello nell'ordinanza con ulteriori disposizioni transitorie. Ad ogni nuovo obbligo che generera un'ingente mole di lavoro andrebbero associati termini transitori adeguati, in particolare per l'obbligo di garantire un'adeguata sicurezza dei dati (art. 8 nLPD in combinato disposto con l'art. 19 AP-OLPD), l'obbligo di tenere un registro delle attività di trattamento (art. 12 nLPD) e l'obbligo di segnalare il più rapidamente possibile le violazioni della sicurezza dei dati (art. 24 nLPD in combinato disposto con l'art. 19 AP-OLPD). Per questi obblighi, sebbene sussistano già oggi, è necessario un termine transitorio almeno fino al 1° luglio 2023.[555]

3.3 Allegato 2

3.3.1 Ordinanza VOSTRA

Il Cantone di Soletta osserva che l'articolo 18 dell'ordinanza VOSTRA[556] prevede che i dati del casellario giudiziale di cui all'articolo 366 capoversi da 2-4 CP possono essere isolati in una nuova banca dati mediante registrazione o conservazione unicamente se questo è necessario per motivare una decisione presa o una pratica procedurale avviata. Tuttavia, con la prevista entrata in vigore della legge sul casellario giudiziale nel 2023, gli uffici cantonali di polizia avranno accesso al casellario giudiziale. Quest'ultimo contiene, tra le altre cose, informazioni sugli allontanamenti e sui divieti di ritorno vigenti secondo il CC e il diritto cantonale. Al fine di prevenire i pericoli e i reati, i dati sono disponibili in particolare per gli agenti di polizia che intervengono sul posto. Secondo il Cantone di Soletta, lo stesso dovrebbe essere possibile anche per i divieti di cui agli articoli 67 e seguenti del CP. Pertanto, il tenore della disposizione andrebbe ampliato, aggiungendo ad esempio che i dati sono necessari anche «per l'esecuzione di una decisione presa».

3.3.2 Allegato alla modifica dell'ordinanza sulle rilevazioni statistiche

Per quanto riguarda l'allegato alla modifica dell'ordinanza sulle rilevazioni statistiche, il Cantone di Vaud osserva che al numero 72 rubrica riga 3 colonna 2 e riga 9 colonna 2 la dicitura «con l'accordo degli interessati» permette di utilizzare certe informazioni per determinati scopi amministrativi. Questo era già contenuto nell'allegato dell'attuale ordinanza sulle rilevazioni stati-

[551] Organizzazioni: ABES, ASA.

[552] Organizzazioni: ABES, economiesuisse, ASB.

[553] Organizzazioni: Economiesuisse, ASB.

[554] Organizzazioni: ABES, santésuisse.

[555] Organizzazioni: Economiesuisse, ASB.

[556] Ordinanza del 29 settembre 2006 sul casellario giudiziale, RS 331.

stiche. Tuttavia, questa possibilità costituisce una deroga importante ai principi fondamentali inerenti al trattamento dei dati statistici. È quindi auspicabile esemplificare ciò che s'intende per «determinati scopi amministrativi».

3.3.3 Ordinanza VIS

FER constata in relazione all'articolo 31 capoverso 1 dell'ordinanza VIS del 18 dicembre 2013[557] che nella versione in lingua francese manca il soggetto "elle". Quindi, la frase dovrebbe essere corretta come segue: "[...], *elle* présente une demande écrite au SEM".

3.3.4 Ordinanza sul collocamento

Per quanto riguarda l'ordinanza del 16 gennaio 1991[558] sul collocamento, FER osserva che l'articolo 19 capoverso 2 lettera c nLPD prevede che, in occasione della raccolta di dati personali, il titolare del trattamento dei dati comunichi alla persona interessata le informazioni necessarie per permetterle di far valere i suoi diritti secondo la legge e per garantire un trattamento trasparente dei dati. Come minimo, il titolare deve comunicare agli interessati «[...] se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali». FER ritiene che la versione francese dell'articolo 58 capoverso 1 lettera d OC dovrebbe riprendere esattamente il tenore della legge. La versione attuale recita «[...] le cas échéant, des destinataires auxquelles des données sont transmises [...]». Tuttavia, sarebbe meglio: «[...] le cas échéant, les destinataires ou les catégories de destinataires auxquels des données personnelles sont transmises».

La lettera a, che obbliga l'autorità preposta al mercato del lavoro di informare le persone in cerca di lavoro e i datori di lavoro che si annunciano sull'«identità e i dati di contatto del ritolare del sistema d'informazione», andrebbe stralciata, poiché non vi è una pertinente base legale. L'articolo 19 capoverso 2 lettera a nLPD menziona solo l'identità e i dati di contatto del titolare del trattamento.

Inoltre, FER afferma che le osservazioni di cui all'articolo 58 OC dovrebbero applicarsi anche all'articolo 126 OADI.[559]

4 Consultazione

Secondo l'articolo 9 della legge federale del 18 marzo 2005[560] sulla procedura di consultazione, i documenti della consultazione, le osservazioni dei partecipanti alla procedura di consultazione, dopo la scadenza del periodo di consultazione, e il rapporto sui risultati, dopo che il Consiglio federale ne ha preso atto, sono accessibili al pubblico. Questi documenti sono disponibili in forma elettronica sul sito web della Cancelleria federale. Sullo stesso sito sono accessibili i pareri dei partecipanti alla consultazione (art. 16 dell'ordinanza del 17 agosto 2005[561] sulla consultazione).

[557] RS **142.512**

[558] RS **823.111**

[559] Ordinanza del 31 agosto 1983 sull'assicurazione obbligatoria contro la disoccupazione e l'indennità per insolvenza, RS 837.02.

[560] RS **172.061**

[561] RS **172.061.1**

5 Glossario

AP-OLPD / E-VDSG / P-OLPD	Avamprogetto dell'ordinanza relativa alla legge federale sulla protezione dei dati / Entwurf zur Verordnung zum Bundesgesetz über den Datenschutz / Projet d'Ordonnance relative à la loi fédérale sur la protection des données
art. / Art. / art.	articolo / Artikel / Article
BCRs	Binding Corporate Rules (norme vincolanti d'impresa)
bzw. / resp.	Beziehungsweise / respectivement
CAID / CIA / CAID	Confidenzialità, autenticità, integrità, disponibilità / Vertraulichkeit, Integrität, Verfügbarkeit / Confidentialité, Authenticité, Intégrité, Disponibilité
cpv. / Abs. / para.	capoverso / Absatz / paragraphe
Direttiva (UE) 2016/680 / Richtlinie (EU) 2016/680 / Directive (UE) 2016/680	Direttiva (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali / Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung / Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales
DTF / BGE / ATF	Decisioni del Tribunale federale / Bundesgerichtsentscheid / Arrêt du Tribunal fédéral
fr.	franco svizzero / Schweizer Franken / Franc suisse
IA / KI / IA	intelligenza artificiale / Künstliche Intelligenz / Intelligence artificielle
ICT	Information and Communication Technology
Id-e / Id-e	Identità elettronica / Elektronische Identität / Identité électronique
IFPDT / EDÖB / PFPDT	L'Incaricato federale della protezione dei dati e della trasparenza / Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte / Le préposé fédéral à la protection des données et à la transparence
IT	Information Technology
lett. / Lit. / Let.	lettera / Litera / Lettre
n. / ziff. / ch.	numero / Ziffer / Chiffre

nLPD / nDSG / nLPD	Legge federale del 25 settembre 2020 sulla protezione dei dati / Bundesgesetz vom 25. September 2020 über den Datenschutz / Loi fédérale du 25 septembre 2020 sur la protection des données
OIN / ISO	Organizzazione Internazionale di normazione / Internationale Organisation für Normung / Organisation internationale de normalisation
OLPD / VDSG / OLPD	Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati / Verordnung zum Bundesgesetz über den Datenschutz (Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz / Ordonnance fédérale du 14 juin 1993 relative à la loi fédérale sur la protection des données
p. es. / z.B. / p. ex.	per esempio / zum Beispiel / par exemple
PMI / KMU / PME	piccola e media impresa / Kleine und mittlere Unternehmen / Petite ou moyenne entreprise
RGPD / DSGVO / RGPD	Regolamento europeo sulla protezione dei dati del 27 aprile 2016 / Datenschutz-Grundverordnung der Europäischen Union vom 27. April 2016 / Règlement européen du 27 avril 2016 sur la protection des données
SA / AG / SA	Società anonima / Aktiengesellschaft / Société anonyme
Sagl / GmbH /Sàrl	Società a garanzia limitata / Gesellschaft mit beschränkter Haftung / Société à responsabilité limitée
TAF / BVGer / TAF	Tribunale amministrativo federale / Bundesverwaltungsgericht / Tribunal administratif fédéral
UE / EU / UE	Unione europea / Europäische Union / Union européenne
VIPD / DSFA / AIPD	Valutazioni d'impatto sulla protezione dei dati / Datenschutz-Folgenabschätzung / Analyses d’impact de protection des données

6 Allegato

Elenco dei partecipanti
Verzeichnis der Eingaben
Liste des organismes ayant répondu

Cantoni / Kantone / Cantons

AG		Argovia / Aargau / Argovie
AI		Appenzello Interno / Appenzell Innerrhoden / Appenzell Rh.-Int.
AR		Appenzello Esterno / Appenzell Ausserrhoden / Appenzell Rh.-Ext.
BE		Berna / Bern / Berne
BL		Basilea-Campagna / Basel-Landschaft / Bâle-Campagne
BS		Basilea-Città / Basel-Stadt / Bâle-Ville
FR		Friburgo / Freiburg / Fribourg
GE		Ginevra / Genf / Genève
GL		Glarone / Glarus / Glaris
GR		Grigioni / Graubünden / Grisons
LU		Lucerna / Luzern / Lucerne
NE		Neuchâtel / Neuenburg
NW		Nidvaldo / Nidwalden / Nidwald
OW		Obvaldo / Obwalden / Obwald
SG		San Gallo / St. Gallen / Saint-Gall
SH		Sciaffusa / Schaffhausen / Schaffhouse
SO		Soletta / Solothurn / Soleure
SZ		Svitto / Schwyz
TG		Turgovia / Thurgau / Thurgovie
TI		Ticino / Tessin
UR		Uri
VD		Vaud / Waadt
VS		Vallese / Wallis / Valais
ZH		Zurigo / Zürich / Zurich

Partiti politici / Parteien / Partis politiques

Alleanza del Centro	Alleanza del Centro Die Mitte Le Centre
PLR	PLR. I Liberali Radicali FDP. Die Liberalen PLR. Les Libéraux-Radicaux PLD. Ils Liberals
PVS	Partito dei Verdi Svizzeri PVS Grüne Partei der Schweiz GPS Parti les VERT-E-S suisse PVS

PPS	Partito pirata Svizzeri PPS Piratenpartei Schweiz PPS Parti pirate suisse PPS
PS	Partito socialista svizzero PS Sozialdemokratische Partei der Schweiz SP Parti socialiste suisse PS
UDC	Unione democratica di centro UDC Schweizerische Volkspartei SVP Union démocratique du centre UDC

Cerchie interessate e privati / Interessierte Organisationen und Privatpersonen / Organisations intéressées et particuliers

ADIDE	Association pour le dictionnaire des droits de l'enfant
ABES	Associazione delle banche estere in Svizzera Association of Foreign Banks in Switzerland Verband der Auslandbanken in der Schweiz Association des banques étrangères en Suisse
UPSA	Unione professionale svizzera dell'automobile Auto Gewerbe Verband Schweiz Union professionelle suisse de l'automobile
IS	Inserimento Svizzera Arbeitsintegration Schweiz Insertion Suisse
ASA	Associazione Svizzera d'Assicurazioni Schweizerischer Versicherungsverband Association Suisse d'Assurances Swiss Insurance Association
ASDPO	Association Suisse des Délégués à la Protection des Données
ASIP	Associazione svizzera delle Istituzioni di previdenza Schweizerischer Pensionskassenverband Association suisse des Institutions de prévoyance
ASPS	Associazione Spitex privata Svizzera
asut	Associazione svizzera delle telecomunicazioni Schweizerischer Verband der Telekommunikation Association Suisse des Télécommunications Swiss Telecommunications Association
ATPrD	Autorité cantonale de la transparence et de la protection des données (Fribourg) Kantonale Behörde für Öffentlichkeit und Datenschutz (Fribourg)
auto schweiz/auto suisse	Associazione degli importatori svizzeri di automobili
Bär & Karrer	Bär & Karrer AG
Beat Lehmann	Avvocato lic. iur.
Bibliosuisse	Bibliosuisse

Classtime	Classtime AG
Coop	Coop Società Cooperativa
CP	Centre Patronal
Creditreform	Creditreform Egeli Vogel Bern AG
curafutura	Gli assicuratori-malattia innovativi Die innovativen Krankenversicherer Les assureurs-maladie innovants
CURAVIVA	CURAVIVA Svizzera CURAVIVA Schweiz CURAVIVA suisse
CYBER SAFE	Association Suisse pour le Label de Cybersécurité
Datenschutzbeauftragter SZ/OW/NW	Responsabile della protezione dei dati Svitto Obvaldo Nidvaldo
Datenschutzguide.ch	Datenschutzguide.ch GmbH c/o gbf Rechtsanwälte AG
DFS	Datenschutz Forum Schweiz
le banche domestiche / die Inlandbanken / les banques domestiques	Associazione delle banche regionali svizzere Unione delle Banche Cantonali Svizzere Banca Migros SA Raiffeisen Svizzera società cooperativa Verband Schweizer Regionalbanken Verband Schweizer Kantonalbanken Migros Bank AG Raiffeisen Schweiz Genossenschaft Les banques domestiques
la Posta / die Post/la Poste	La Posta Svizzera SA
DigiGes	Società digitale Digitale Gesellschaft Société numérique
digitalswitzerland	Iniziativa digitalswitzerland
economiesuisse	Federazione delle imprese svizzere Verband der Schweizer Unternehmen Fédération des entreprises suisses Swiss Business Federation
CFC	Commissione federale del consumo Eidgenössische Kommission für Konsumentenfragen Commission fédérale de la consommation CFC
Biblioteca dell'ETH	Biblioteca del Politecnico federale di Zurigo
EXPERTsuisse	EXPERT SUISSE revisione dei conti / tasse / amministrazione fiduciaria
FER	Fédération des Entreprises Romandes

FMH	Federazione dei medici svizzeri Verbindung der Schweizer Ärztinnen und Ärzte Fédération des médecins suisses Foederatio Medicorum Helveticorum
Forum PMI	Forum PMI Forum PME KMU-Forum
FRC	Fédération romande des consommateurs
GastroSuisse	Per l'Albergheria e la Ristorazione Für Hotellerie und Restauration Pour l'Hôtellerie et la Restauration
H+	Gli ospedali Svizzeri Die Spitäler der Schweiz Les hôpitaux de suisse
HÄRTING Rechtsanwälte/HÄRTING	HÄRTING Rechtsanwälte AG
ASSOCIAZIONE DI COMMERCIO.swiss	Associazione di commercio Handelsverband Association de commerce
HKBB	Handelskammer beider Basel
HDC	HDC law firm étude d'avocats
HotellerieSuisse	Associazione svizzera albergheria Schweizerischer Hotellerie Verband
IGEM	Interessengemeinschaft elektronische Medien
INSOS	INSOS Schweiz
Migros	Cooperativa Migros
EPS	Educazione Privata Svizzera Private Bildung Schweiz Swiss Private Education Education Privée Suisse
pharmaSuisse	Associazione svizzera dei farmacisti
Préposé cantonal à la protection des données et à la transparence NE/JU	Incaricato cantonale della protezione dei dati e della trasparenza dei Cantoni di Neuchâtel e Giura
Privacy Icons	Privacy Icons c/o Wenger & Vieli AG
privatim	Conferenza degli incaricati svizzeri per la protezione dei dati Konferenz der schweizerischen Datenschutzbeauftragten Conférence des préposé(e)s suisse à la protection des données
proFonds	Associazione mantello delle fondazioni non profit svizzere

Raiffeisen	Banca Raiffeisen Raiffeisenbank Banque Raiffeisen
rega	Guardia aerea svizzera di soccorso Schweizerische Rettungsflugwacht Garde aérienne suisse de sauvetage
Ringier	Ringier AG Ringier SA
ASP	Associazione svizzera del pneumatico Reifen-Verband der Schweiz Association Suisse du Pneu
santésuisse	Le assicurazioni malattia svizzere Die Schweizer Krankenversicherer Les assureus-maladie suisses
USI	Unione svizzera degli imprenditori USI Schweizerischer Arbeitgeberverband SAV Union patronale suisse UPS L'Unione svizzera degli imprenditori, secondo una ripartizione dei dossier con economiesuisse, non ha espresso alcun parere, quindi alla sigla tedes SAV è sempre da intendersi Federazione Svizzera degli Avvocati.
FSA	Federazione Svizzera degli Avvocati Schweizerischer Anwaltsverband Fédération Suisse des Avocats Swiss Bar Association
FFS	FFS SBB CFF
ASB	Associazione Svizzera dei Banchieri Schweizerische Bankiervereinigung Association suisse des banquiers Swiss Bankers Association
Scienceindustries Switzerland	Associazione di categoria dell'industria chimica, farmaceutica e delle scienze della vita Wirtschaftsverband Chemie Pharma Life Sciences
SDV	Associazione Svizzera di Marketing Dialogo
senesuisse	Associazione svizzera degli istituti per anziani e di cura economicamente indipendenti Verband wirtschaftlich unabhängiger Alters- und Pflegeeinrichtungen Schweiz Association d'établissements économiquement indépendants pour presonnes âgées Suisse
UPSC/SFF/UPSV	Unione Professionale Svizzera della Carne Schweizer Fleischfachverband Union Professionelle Suisse de la Viande
USS	Unione sindacale svizzera Schweizerischer Gewerkschaftsbund Union syndicale suisse Unions sindicale svizzera

usam	Unione svizzera delle arti e mestieri Schweizerischer Gewerbeverband Union suisse des arts et métiers
ASSL	Associazione svizzera delle società di leasing Schweizerischer Leasingverband Association Suisse des Sociétés de Leasing
BNS	Banca Nazionale Svizzera Schweizerische Nationalbank Banque Nationale Suisse Banca Naziunala Svizera Swiss National Bank
SPA	Swiss Payment Association
Spitex Svizzera	Assistenza e cura a domicilio Dachverband der Schweizer Nonprofit-Spitex Aide et soins à domicile suisse
SSO	Società svizzera odontoiatri Schweizerische Zahnärzte-Gesellschaft Société suisse des médecins-dentistes Swiss Dental Association
UCS	Unione delle città svizzere Schweizerischer Städteverband Union des villes suisses
SKS	Fondazione per la protezione dei consumatori Stiftung für Konsumentenschutz
SUISA	Cooperativa degli autori ed editori di musica Genossenschaft der Urheber und Verleger von Musik Coopérative auteurs et éditeurs de musique
Sunrise UPC	Sunrise UPC Sagl
suva	Istituto nazionale svizzero di assicurazione contro gli infortuni
SWICO	Associazione di categoria dell'industria ICT e online
Swimag	Swimag GmbH
SwissFoundations	Associazione delle fondazioni donatrici svizzere Association of swiss grant-making foundations Verband der Schweizer Förderstiftungen Association des fondations donatrices suisses
SwissHoldings	Federazione svizzera dei gruppi industriali e dei servizi
swissICT	Associazione di categoria ICT
Swiss Insights	Swiss Data Insights Association
swissprivacy.law	swissprivacy.law
swissstaffing	Associazione dei fornitori di servizi per il personale
thurbo	thurbo AG ferrovia regionale
veb.ch	Associazione per la presentazione dei conti, il controllo di gestione e la contabilità

UTP	Unione dei trasporti pubblici Verband öffentlicher Verkehr Union des transports publics
vsi	Verband Schweizerischer Inkassotreuhandinstitute (Società di recupero crediti)
UBCS	Unione delle Banche Cantonali Svizzere Verband Schweizerischer Kantonalbanken Union des Banques Cantonales Suisses
VSP	Federazione svizzera delle scuole private Verband Schweizerischer Pritvatschulen Fédération suisse des écoles privées
VUD	Verein Unternehmens-Datenschutz (Associazione protezione dei dati aziendali)
Walderwyss	Walder Wyss AG

Rapporto sui risultati della procedura di consultazione: revisione totale dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD)

Tribunali federali / Eidgenössische Gerichte / Tribunaux de la Confédération

Tribunale amministrativo federale / TAF	Tribunale amministrativo federale Tribunal administratif fédéral Bundesverwaltungsgericht

Rinuncia a un parere / Verzicht auf Stellungnahme / Renonciation à une prise de position

- JU, ZG, NE, TI
- Conferenza dei Governi Cantonali (CdC)
- Unione Democratica Federale UDF
  Eidgenössisch-Demokratische Union EDU
  Union Démocratique Fédérale UDF
- Ensemble à Gauche EAG
- Partito evangelico svizzero PEV
  Evangelische Volkspartei der Schweiz EVP
  Parti évangélique suisse PEV
- Partito verde liberale svizzero pvl
  Grünliberale Partei Schweiz glp
  Parti vert'libéral Suisse pvl
- Lega dei Ticinesi (Lega)
- Partito Operaio e Popolare POP
  Partei der Arbeit PDA
  Parti suisse du travail PST
- Associazione dei Comuni Svizzeri
  Schweizerischer Gemeindeverband
  Association des Communes Suisses
- Gruppo svizzero per le regioni di montagna
  Schweizerische Arbeitsgemeinschaft für die Berggebiete
  Groupement suisse pour les régions de montagne
- Unione svizzera degli imprenditori
  Schweizerischer Arbeitgeberverband
  Union patronale suisse
- Svizzera. Unione svizzera dei contadini (USC)
  Bauernverband (SBV)
  Union suisse des paysans (USP)
- Società svizzera degli impiegati di commercio
  Kaufmännischer Verband Schweiz
  Société suisse des employés de commerce

- Travail.Suisse

- Tribunale penale federale
  Bundesstrafgericht
  Tribunal pénal fédéral

- Tribunale federale svizzero
  Schweizerisches Bundesgericht
  Tribunal fédéral suisse

- Unione svizzera degli imprenditori
  Schweizerischer Arbeitgeberverband
  Union patronale suisse

- Comitato internazionale della Croce Rossa (CICR)

- Associazione consumatrici e consumatori della Svizzera italiana ASCI

- Forum svizzero dei consumatori kf

- Commissione federale del consumo CFC