

29° Rapporto d'attività 2021/22
Incaricato federale della protezione
dei dati e della trasparenza



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapporto d'attività 2021/2022

dell'Incaricato federale della protezione dei dati e della trasparenza

L'Incaricato fa rapporto all'Assemblea federale periodicamente e secondo i bisogni.
Trasmette contemporaneamente il rapporto al Consiglio federale (art. 30 LPD).

Il presente rapporto riguarda il periodo dal 1° aprile 2021 al 31 marzo 2022.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Premessa

Nella speranza che la pandemia, con i suoi problemi sanitari e le sue limitazioni della libertà, sia giunta al capolinea, con l'app COVID e il certificato COVID, inclusa la sua versione light, la Svizzera digitale fa segnare successi di tutto rispetto sotto il profilo della protezione dei dati. Grazie alla concezione decentralizzata e alla quantità di dati ridotta al minimo di questi strumenti digitali, è stato possibile evitare il trasferimento di dati di cittadini all'Amministrazione federale e contenere in misura accettabile sotto il profilo della protezione dei dati la divulgazione di dati sanitari nei confronti di privati.

Allo stesso tempo la Svizzera digitale si lecca le ferite provocate dal malfunzionamento tecnico e organizzativo di determinate applicazioni per il contact tracing o di registri di vaccinazioni, donazioni di organi e protesi mammarie. Al più tardi da quando il giornalismo investigativo ha rivelato al grande pubblico con quale facilità persone non autorizzate riescono a trattare dati personali sensibili, tutti i gestori di piattaforme si sono resi conto di doversi assumere di propria iniziativa le proprie responsabilità. È significativo che, dopo tanto tergiversare, la realizzazione di un'identità elettronica riconosciuta dallo Stato debba riuscire al secondo tentativo.

Sotto la spinta della pandemia, la digitalizzazione del nostro mondo del lavoro e delle attività del tempo libero ha conosciuto un'accelerazione. Con l'annuncio «metaverso» è stato inoltre dato avvio ai lavori per la sostituzione delle attuali piattaforme sociali basate su app. Nell'interconnessione di nuova generazione basata su Internet, le persone potranno incontrarsi mediante leggerissimi occhiali VR in luoghi virtuali nei quali il loro ambiente fisico si sovrappone a segnali digitali trasformandosi in tal modo in un mondo «migliorato». Come rileveranno il nostro ambiente privato questi occhiali VR? E le intelligenze artificiali come percepiranno e interpreteranno nel cloud la nostra mimica, le nostre voci e l'intero nostro comportamento? Prima o poi le persone percepiranno il mondo naturale, non registrato, come grigio, solitario e minaccioso?

Queste questioni concernenti la vigilanza sulla protezione dei dati da parte della Confederazione esprimono la richiesta della popolazione di partecipare alla definizione della realtà digitale di domani.

Adrian Lobsiger

Incaricato federale della protezione dei dati e della trasparenza



Berna, 31 marzo 2022

Sfide attuali 6

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali 14

- L'IFPDT si è adoperato per attuare conformemente alla protezione dei dati numerosi progetti di digitalizzazione della Confederazione
- Legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità
- L'IFPDT esprime critiche sulla rilevazione dei dati fiscali
- Analisi del trattamento dei dati

Tema prioritario I 18

Lavori in vista dell'entrata in vigore della LPD riveduta

- Chiesta una nuova soluzione statale
- Trasparenza del finanziamento della vita politica
- La Confederazione sviluppa una rete di know-how basata sull'AI

1.2 Giustizia, polizia, sicurezza 26

- Istituzione dell'Ufficio federale della dogana e della sicurezza dei confini
- La revisione deve garantire lo stesso livello di trasparenza della LAIn attuale
- Richieste di verifica in caso di differimento
- Attività di coordinamento a livello nazionale

1.3 Commercio ed economia 31

- Diem ritira in Svizzera il progetto per un sistema di pagamento tramite blockchain
- La trasmissione di dati all'autorità statunitense di vigilanza sulle borse è per principio ammissibile
- Trattamento di dati dei clienti
- Piattaforma d'aste Ricardo: nuovi sviluppi nella procedura
- Accertamenti presso una società di leasing per auto
- Inchiesta su un possibile uso improprio dell'accesso al sistema di segnalazione SS7
- I nuovi termini di servizio di WhatsApp destano preoccupazioni in fatto di protezione dei dati
- Progetto degli editori di media svizzeri per un accesso comune a portali in rete
- Completamento automatico dei dati del conto
- Registrazioni errate nella banca dati di una società di riscossione
- Nuova tessera di membro con funzione di carta di credito integrata per i tiratori

1.4 Salute 41

- Accompagnamento del progetto per un certificato COVID-19 conforme alla protezione dei dati e per il certificato «light»
- Accertamento dei fatti concernente l'applicazione SocialPass
- Inchiesta concernente la piattaforma di certificati di vaccinazione
- Consultazione, conservazione e cancellazione dei dati dei pazienti
- Vulnerabilità dei registri di donazione di organi e delle protesi mammarie

1.5 Lavoro 49

- Accertamenti presso l'Ufficio federale di statistica riguardanti la conservazione in forma cartacea dei dossier personali

1.6 Assicurazioni 50

- Chiarimento dei ruoli e delle competenze tra l'UFSP e l'IFPDT

1.7 Trasporti 52

- Lacune nella sicurezza dei portali clienti
- Consultazione degli uffici relativa alla nuova legge sui dati dei passeggeri aerei
- Parchimetri digitali con inserimento del numero di targa
- Consultazione degli uffici relativa alla revisione parziale della legge sulla circolazione stradale
- Per lo scambio di dati sulla mobilità è necessaria una base legale

1.8 Internazionale 57

- Protezione della vita privata dei bambini nell'ambiente digitale e linee guida relative alla profilazione e nell'ambito di campagne politiche
- Migliorare la collaborazione con le autorità preposte alla protezione dei dati
- Incontro virtuale di oltre 90 membri e osservatori
- Protezione dei dati nell'aiuto internazionale allo sviluppo
- Gruppi di coordinamento di vigilanza dei sistemi SIS II, VIS ed Eurodac
- Buone pratiche delle autorità incaricate della protezione dei dati

Tema prioritario II 64

Comunicazione di dati all'estero

Principio di trasparenza

2.1 In generale.....	70
2.2 Domande di accesso. Nuovo aumento nel 2021.....	72
2.3 Procedure di mediazione: aumento significativo delle domande di mediazione.....	76
– Percentuale di soluzioni consensuali	
– Durata delle procedure di mediazione	
– Numero di casi pendenti	
2.4 Procedura legislativa.....	81
– Revisione della legge federale sulle attività informative	

L'IFPDT

3.1 Compiti e risorse.....	84
– Pandemie	
– Prestazioni e risorse nell'ambito della protezione dei dati	
– Partecipazione a deliberazioni delle commissioni e audizioni da parte di commissioni parlamentari	
– Prestazioni e risorse nell'ambito della legge sulla trasparenza	
3.2 Comunicazione.....	88
– Principali temi dell'attività di comunicazione	
– Crescente attenzione da parte dei media e della popolazione	
– Rapporto d'attività e sviluppo di un nuovo sito Internet	
3.3 Statistiche.....	90
– Statistiche sulle attività dell'IFPDT dal 1° aprile 2021 al 31 marzo 2022 (Protezione dei dati)	
– Panoramica delle domande d'accesso dal 1° gennaio al 31 dicembre 2021	
– Statistica delle domande d'accesso secondo la legge sulla trasparenza dal 1° gennaio al 31 dicembre 2021	
– Domande di accesso 2021 con riferimento a Corona	
– Numero di domande di mediazione secondo la categoria di richiedenti	
– Trattamento delle domande d'accesso dal 1° gennaio al 31 dicembre 2021	
3.4 Organizzazione IFPDT.....	100
– Organigramma	
– Personale dell'IFPDT	
Abbreviazioni.....	102
Indice figurativo.....	103
Impressum.....	104
Nel pieghevole	
– Cifre chiave	
– Preoccupazioni relative alla protezione dei dati	

Sfide attuali

I Digitalizzazione

In Svizzera quasi tutte le persone entrano quotidianamente in contatto con tecnologie dell'informazione e della comunicazione (TIC). La digitalizzazione è penetrata nella nostra società. Questo sviluppo non è però destinato a raggiungere un punto di saturazione, bensì a proseguire come processo di progressiva rielaborazione di realtà digitali.

Lo smartphone raggiungerà presto il culmine delle sue potenzialità?

Il processo di progressiva rielaborazione di realtà digitali si lascia ben illustrare con l'esempio degli smartphone, che negli ultimi quindici anni hanno svolto un ruolo di primo piano nella penetrazione digitale della società. Nel periodo in rassegna la produzione di dati attraverso questo dispositivo si è ulteriormente intensificata, visto che per mesi l'accesso a manifestazioni pubbliche e ristoranti è dipeso dalla presentazione di un certificato COVID-19 e che è oramai invalsa l'abitudine di portare sempre con sé lo smartphone acceso durante gli spostamenti nello spazio pubblico. D'altra parte, il dibattito sempre più intenso nei media sulla visione del cosiddetto «metaverso» lascia intendere che anche lo smartphone lascerà il passo: secondo i fautori di questa visione le persone si allontaneranno gradualmente dalle

attuali piattaforme basate su app, compresi schermi, mouse e tastiere, per entrare in spazi virtuali indossando un paio di semplici occhiali.

Tra «metaverso» e mondo reale

Nel periodo in rassegna, per attrarre investitori e utenti per la propria parte del futuro «metaverso» a diffusione mondiale e per stabilirvi diritti commerciali, il gruppo di comunicazione globale facebook ha modificato il proprio nome in «Meta».

Nell'interconnessione di nuova generazione basata su Internet, le persone potranno incontrarsi mediante leggerissimi occhiali VR in luoghi virtuali nei quali il loro ambiente fisico si sovrappone a segnali digitali trasformandosi in tal modo in un mondo misto, migliorato o una «realtà aumentata». Le persone dovrebbero percepire questo nuovo ambiente a livello sensoriale come reale, anche se gli avatar digitali attraverso i quali si incontrano nel «metaverso» non sono in carne e ossa. Questi incontri si svolgeranno anche in abitazioni private e locali commerciali. Per renderli possibile, i sensori scansioneranno e misureranno le pareti private e diffonderanno i dati così ottenuti in tempo reale via Internet. Già questo

fa capire come il concetto di «metaverso» implichi un'ingerenza nella sfera privata di miliardi di persone.

Tutti dovrebbero essere in grado di immergersi in pochi secondi nel «metaverso» semplicemente indossando occhiali poco appariscenti. Che cosa questo comporti per la permanenza nel mondo naturale, senza animazioni digitali, può essere desunto dal comportamento dei consumatori di giochi virtuali. Quando, prima o poi, le persone percepiranno il mondo reale, puro e semplice, senza alcun elemento digitale, come grigio e solitario, è probabile che vi rimarranno molto meno. Un giorno la meta-società arriverà a considerare una passeggiata nel mondo senza animazioni digitali come una minaccia per sé stessi, perché nel mondo naturale mancano determinati avvisi di pericolo?

Per mettere in scena la «realtà aumentata» gli occhiali VR e i loro sensori registreranno gli sguardi, la mimica, le voci e le posture, fino alle letture e al cibo ingerito da chi li porta. Tutti questi dati sensibili finiranno prima o poi nel cloud dei gestori di social network – e questo, ovviamente, in misura esponenzialmente maggiore di quanto già non avviene nella realtà digitale di oggi.

Più le persone trasferiscono le loro vite sociali in mondi animati digitalmente, più alta è purtroppo la probabilità che la loro sfera personale sia violata. Questo è il caso, ad esempio, quando si utilizzano avatar fotorealistici, il cui perfezionamento è oramai soltanto una questione di tempo. In questo contesto, l'IFPDT si adopererà sin dall'inizio, in collaborazione con altre autorità di vigilanza, per garantire che i fornitori

«Il concetto di «metaverso» implica un'ingerenza nella sfera privata di miliardi di persone.»

dei mondi animati digitalmente rendano trasparenti i rischi che questi comportano e adottino misure per proteggere la sfera privata e l'autodeterminazione degli utenti.

Strategia «Svizzera digitale»

Per garantire che la popolazione svizzera possa beneficiare dei vantaggi della digitalizzazione, il Consiglio federale elabora periodicamente la strategia «Svizzera digitale». Tale strategia incoraggia le autorità a tutti i livelli istituzionali, nonché la società civile, le imprese, la scienza e la politica, a promuovere congiuntamente la trasformazione digitale.

Secondo la strategia «Svizzera digitale», la trasformazione digitale delle strutture esistenti esige un cambiamento di mentalità che rimette in discussione le forme tradizionali di convivenza e di economia. Le competenze digitali e la messa in rete nonché la condivisione di dati tra tutti gli attori sono all'ordine del giorno. Dall'accumulo di conoscenze che ne risulta deve nascere una Svizzera in cui, anche nello spazio digitale, la popolazione partecipa alla vita sociale, politica ed economica.

Servizio pubblico come partner discreto della popolazione

Secondo molti fautori del cambiamento digitale, agli antipodi di questa visione strategica vi è la malvista conservazione di dati in cosiddetti silos, associata a un modo di pensare superato e allo stereotipo di un'amministrazione bernese che guarda al passato. A tal proposito si trascura purtroppo con troppa leggerezza che barriere nella trasmissione delle informazioni apparentemente obsolete possono costituire pilastri interni del sistema del moderno Stato di diritto. Questo ha preso il posto delle signorie dell'aristocrazia, nelle quali tutte le attività sovrane derivavano dal potere di un principe. Quest'ultimo poteva avocare a sé qualsiasi affare in qualsiasi momento, prendere conoscenza di qualsiasi informazione ed evadere tale affare adottando una decisione sul suddito interessato in modo del tutto personale. È soltanto con la costituzione secondo i principi dello Stato di diritto di un sistema giudiziario separato e indipendente e la diversificazione dell'amministrazione in uffici specializzati dotati

di conoscenze esclusive che furono create le condizioni affinché lo Stato diventasse un servizio pubblico e i sudditi diventassero cittadini.

Oggi, lo Stato fondato sulla suddivisione dei poteri si presenta come un conglomerato di servizi che forniscono prestazioni che aiutano la popolazione ad esercitare i diritti e i doveri civili stabiliti in speciali leggi. La specializzazione dell'amministrazione e la segmentazione delle informazioni ufficiali sono procedute di pari passo con una trasformazione del potere statale sulla società civile, la quale oggi fa valere con consapevolezza i suoi diritti e richiede agli uffici specializzati, in cambio delle imposte versate, servizi professionali e discreti e, se necessario, li fa valere in tribunale.

Lo Stato di diritto si concentra sulla messa in rete di dati fattuali anziché di dati dei cittadini

In questo contesto storico, la protezione dei dati deve sostenere in modo differenziato l'esigenza strategica di coinvolgere sempre più lo Stato e l'amministrazione nella diffusione, condivisione e uso dei dati nella rete digitale. La protezione dei dati deve prodigarsi affinché questa dinamizzazione delle

«Quando le persone percepiranno il mondo reale, senza alcun elemento digitale, come grigio e solitario, è probabile che vi rimarranno molto meno.»

informazioni non si concentri su dati personali, bensì su dati fattuali e avvenga nel rispetto dei limiti informativi conformemente allo Stato di diritto che consentono alla società civile di far valere i propri diritti civili nei confronti delle autorità.

La protezione dei dati riguarda la salvaguardia di diritti fondamentali che negli Stati autoritari sono negati, perché in tali Stati ancora oggi le persone devono mettere in conto il fatto che, a causa di una quantità di informazioni e fonti di dati statali a loro incomprensibili, l'amministrazione limita loro l'accesso agli uffici, ai sussidi o all'istruzione, comprese le prestazioni sociali e le cure mediche. Attraverso la rete digitale e una tecnologia di sorveglianza a basso costo, gli Stati autoritari hanno ora intensificato il controllo sulla popolazione in una misura che, si spera, continuerà a spaventare l'Occidente per lungo tempo. La Commissione europea si è sentita in dovere, nel progetto per una legislazione sull'intelligenza artificiale, di vietare agli Stati membri dell'UE la sorveglianza sociale continua della popolazione nel senso di un «social scoring» e l'uso in tempo reale a livello nazionale dei sistemi di riconoscimento facciale negli spazi pubblici.

La comunicazione anonima è un diritto civile e mai un «abuso di libertà»

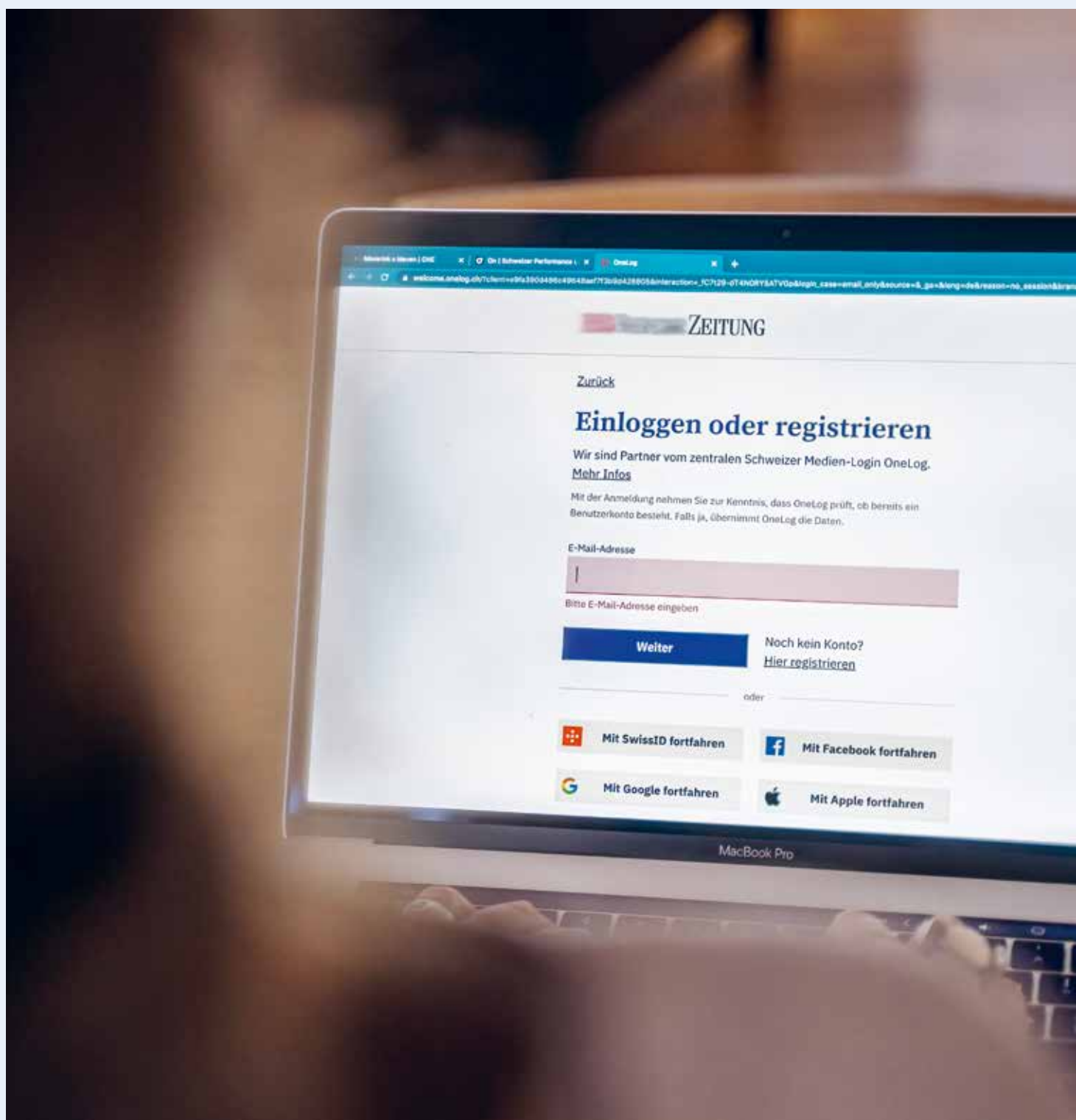
Dal punto di vista della protezione dei dati, è altrettanto importante che nelle democrazie occidentali resti preservato il diritto dei privati di trattare i propri dati e quelli dei propri clienti in modo autonomo e di isolarli a propria discrezione da terzi e quindi anche dallo Stato. L'esistenza della criminalità è intrinseca alla società e pertanto non costituisce mai un motivo valido per addossare ai cittadini l'insostenibile accusa di «abusare della loro libertà» quando comunicano attraverso sistemi a prova di intercettazioni. Se una persona si reca dapprima a piedi in un ristorante e poi in autobus nel luogo in cui successivamente commette un crimine intenzionale, non può essere accusata di movimento abusivo negli spazi pubblici, né di assunzione abusiva di cibo e neppure di uso improprio dei trasporti pubblici. Lo stesso vale

se un criminale scambia informazioni tramite canali a prova di intercettazioni prima o dopo aver commesso un atto. Nel mondo libero, ogni persona dovrebbe avere il diritto di muoversi in modo anonimo nel mondo analogico e digitale senza essere incolpato dalle proprie dichiarazioni. E in questo mondo non devono essere ammessi i gruppi tecnologici che, sfruttando l'intelligenza artificiale, ispezionano i telefoni da loro venduti alla ricerca di contenuti illegali per denunciarne i proprietari alla polizia.

Ovviamente, il diritto a una comunicazione anonima non impedisce che in casi puntuali la polizia possa intervenire nei confronti di persone, e del loro entourage, sospettate di aver commesso un reato, purché con l'autorizzazione del giudice.

Se in Svizzera sarà invece impedito ai privati, senza requisiti legali sufficientemente chiari, di proteggere da tutti le loro informazioni private e quelle dei loro clienti, l'IFPDT vi si opporrà nell'ambito delle sue competenze legali. A tal proposito l'IFPDT chiede che le strategie digitali siano attuate in modo differenziato e con prudenza al fine di consolidare la sfera privata e l'autodeterminazione della popolazione svizzera, piuttosto che di indebolirle.

«La protezione dei dati riguarda la salvaguardia di diritti fondamentali che sono negati alle persone negli Stati autoritari.»



II Attività di consulenza, controllo e mediazione

Affinché possa, nella sua veste di autorità di vigilanza, assicurare che i dati personali siano trattati non in base alle capacità tecniche bensì all'intensità legalmente consentita, l'IFPDT chiede ai responsabili delle applicazioni digitali di ridurre al minimo, già allo stadio pianificatorio e progettuale, i rischi elevati per la protezione dei dati e di fornire la pertinente documentazione all'autorità di vigilanza in materia di protezione dei dati e ai relativi responsabili aziendali. Seguendo questo orientamento abbiamo portato avanti la nostra consulenza nell'ambito della vigilanza legale su un numero notevole di progetti di big data di autorità federali e imprese private, promuovendo un impiego autoresponsabile di strumenti di lavoro moderni quali la valutazione dell'impatto sulla protezione dei dati nonché la figura del responsabile aziendale della protezione dei dati.

La vigilanza può soddisfare solo parzialmente le legittime aspettative del pubblico

Dopo la netta diminuzione registrata nel periodo 2015/16, le spese relative ai compiti di controllo sono leggermente aumentate negli ultimi anni stabilizzandosi tuttavia su un livello basso a causa della scarsa dotazione di mezzi. Anche nell'anno in rassegna l'IFPDT non ha potuto soddisfare nella misura auspicata le legittime aspettative del pubblico (cfr. n. 3.1). Anche se nell'anno in rassegna ha potuto approfondire la sua buona collaborazione con il Centro nazionale per la cibersicurezza, l'IFPDT non dispone di fondi sufficienti per effettuare sistematicamente prove di campionatura e controlli della sicurezza tecnica che si rivelerebbero particolarmente utili proprio nell'ambito dell'archiviazione di dati sensibili sulla salute. A tal proposito vanno ricordati il caso della Fondazione «mievaccinazioni», ora in liquidazione, e i casi emersi nell'anno in rassegna sugli accessi incontrollati al registro per la donazione di organi e al registro per le protesi mammarie (cfr. n. 1.4).

L'aumento delle richieste di mediazione porta a ritardi nel disbrigo delle procedure

Nella sua funzione di Incaricato della trasparenza, nel periodo in rassegna l'IFPDT ha dovuto sospendere temporaneamente le sue attività di mediazione orale a causa della pandemia, ciò che ha comportato una diminuzione delle soluzioni consensuali. L'IFPDT ha pertanto dovuto redigere più raccomandazioni scritte e, visto il simultaneo aumento delle richieste di mediazione, con le risorse di personale disponibili in molti procedimenti i termini legali sono stati superati. Considerato che le richieste di mediazione tendono ad aumentare, v'è da ritenere che, senza risorse supplementari, questa evoluzione negativa peggiorerà ulteriormente e che il disbrigo rapido dei procedimenti richiesto dal legislatore sarà nuovamente disatteso.

«Le strategie digitali devono essere attuate in modo differenziato e prudente. La digitalizzazione dovrebbe consolidare la sfera privata e l'autodeterminazione della popolazione svizzera, piuttosto che indebolirle.»

III Cooperazione nazionale e internazionale

Cooperazione nazionale

Con la crescente digitalizzazione, la tematica cloud è all'ordine del giorno sia dell'IFPDT sia delle autorità cantonali di protezione dei dati. L'ufficio di privatim, l'Associazione degli incaricati svizzeri della protezione dei dati, ha rielaborato perciò completamente il suo promemoria sui rischi e sulle misure specifiche del cloud e ha adottato la nuova versione nel febbraio 2022. Precedentemente l'IFPDT si era pronunciato sul progetto con voto consultivo. Anche in questo caso la collaborazione è stata buona grazie all'affiatamento tra le persone. Il tema ha impegnato l'IFPDT soprattutto in relazione al cloud nell'Amministrazione federale (cfr. n. 1.1).

Consiglio d'Europa

L'IFPDT continua a impegnarsi attivamente presso il Consiglio d'Europa. Ha perciò partecipato a tutte le sedute del Comitato consultivo della Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (Convenzione 108). Nel 2021 il Comitato dei Ministri del Consiglio d'Europa ha adottato due documenti di cui si era occupato il Comitato consultivo summenzionato: la dichiarazione della tutela del diritto dei minori alla privacy nell'ambiente digitale nonché la modifica della raccomandazione del Comitato dei Ministri concernente la profilazione.

Cooperazione internazionale

La questione della trasmissione di dati personali in un Paese privo di un livello adeguato di protezione è un argomento che solleva simili domande in diversi Stati. In questo contesto, l'IFPDT segue in particolare l'evoluzione in atto nell'UE e negli Stati membri dell'UE e del SEE. L'IFPDT ha così analizzato soprattutto le clausole contrattuali

standard modificate e pubblicate dalla Commissione europea e verificato fino a che punto può riconoscerle anche in Svizzera (cfr. n. 1.8).

Valutazione del livello di protezione dei dati

L'atteso rapporto della Commissione europea concernente l'adeguatezza del livello di protezione dei dati della Svizzera ha subito ulteriori ritardi. Nel frattempo continua a rimanere in vigore l'attuale decisione di adeguatezza della Commissione europea adottata ancora in base alla direttiva 95/46/CE sulla tutela dei dati personali, sostituita dal regolamento generale sulla protezione dei dati (GDPR). Presumibilmente la Commissione europea pubblicherà i rapporti sull'adeguatezza di tutti gli Stati già reputati adeguati secondo il GDPR simultaneamente. Si auspica che ciò accada ancora nel corso del 2022.

Protezione dei dati

1.1 Digitalizzazione e diritti fondamentali

TRASFORMAZIONE DIGITALE DELL'AMMINISTRAZIONE FEDERALE

L'IFPDT si è adoperato per attuare conformemente alla protezione dei dati numerosi progetti di digitalizzazione della Confederazione

L'elevato numero di progetti di trasformazione digitale dell'Amministrazione federale rappresenta una sfida per l'IFPDT, in quanto autorità di piccole dimensioni. Nell'ambito della sua attività di consulenza e vigilanza l'IFPDT si adopera affinché gli aspetti relativi alla legislazione sulla protezione dei dati siano tenuti in considerazione sistematicamente e precocemente. Nell'esercizio di questa funzione si tiene in contatto con il nuovo settore «Trasformazione digitale e governance delle TIC» (TDT) della Cancelleria federale, con l'Ufficio federale dell'informatica (UFIT) e con gli uffici federali responsabili dei progetti, in modo da essere informato tempestivamente sui progetti di digitalizzazione e aggiornato sui progetti previsti e in corso.

La strategia cloud dell'Amministrazione federale, intesa a consentire l'impiego di servizi cloud, è un aspetto importante della trasformazione digitale. L'IFPDT ha espresso il suo parere in merito a interventi parlamentari concernenti l'aggiudicazione di servizi

cloud a imprese americane e cinesi, nonché all'impiego di servizi cloud di Microsoft. Ha inoltre formulato requisiti in materia di protezione dei dati per l'uso del cloud da parte delle autorità pubbliche (cfr. Tema prioritario II).

Dopo che il 7 marzo 2021 la legge sull'identità elettronica (Legge sull'Ie) è stata respinta in votazione popolare, il DFGP ha avviato senza indugio un progetto legislativo per una nuova concezione di identità elettronica. L'IFPDT ha colto l'occasione per dare impulsi sul piano specialistico, esprimendosi anche pubblicamente sulle questioni da lui ritenute più importanti (cfr. n. 1.1).

Il progetto di «Legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA)» intende incentivare lo svolgimento elettronico dei processi aziendali della Confederazione («digital first»). Nell'ambito della consultazione degli uffici, l'IFPDT si è espresso criticamente su diversi disciplinamenti. In particolare, siamo riusciti a ottenere adeguamenti per quanto concerne i

progetti pilota, la garanzia di un livello adeguato di sicurezza dei dati, la responsabilità e gli accessi a fini statistici da parte dell'Ufficio federale di statistica (cfr. n. 1.1).

I dati devono essere registrati possibilmente una sola volta e utilizzati e condivisi più volte (principio «once only» e utilizzo multiplo). Le riserve espresse dall'IFPDT – di cui si è tenuto conto – in merito al progetto pilota per la rilevazione dei dati fiscali, hanno evidenziato con chiarezza che, oltre alle opportunità, sussistono anche rischi per la popolazione (cfr. n. 1.1).

Progetti settoriali specifici

Nei grandi progetti di digitalizzazione settoriali con elevati rischi dal profilo della protezione dei dati rientrano la revisione totale della legge sulle dogane e la revisione parziale della legge federale sulle attività informative (LAI). Entrambi i progetti prevedono in particolare una modernizzazione dei sistemi d'informazione. Nell'ambito di un monitoraggio intensivo del progetto di dogana informatizzata (e-customs), è stato possibile ottenere notevoli miglioramenti dal profilo della protezione dei dati (cfr. n. 1.2). Anche

TRASFORMAZIONE DIGITALE

per quanto concerne la LAIn, l'IFPDT è riuscito a imporre numerosi adeguamenti nel processo di consultazione (cfr. n. 1.2).

Il progetto di digitalizzazione sicuramente più importante nel settore sanitario è quello dell'attuazione della cartella elettronica del paziente, che ha subito importanti ritardi. L'IFPDT accompagna i lavori di attuazione e intrattiene contatti regolari con le autorità competenti e gli attori privati in merito alle sfide relative alla protezione dei dati. Nell'ambito delle consultazioni si è espresso sull'ulteriore sviluppo delle basi legali e dei sistemi.

I rischi dal profilo della protezione dei dati della trasformazione digitale non si limitano alla popolazione, ma riguardano anche i dipendenti dell'Amministrazione federale. Per quanto riguarda un progetto pilota previsto per una rete di know-how, l'IFPDT si è pronunciato sulle condizioni quadro concernenti la legislazione sulla protezione dei dati e sull'ulteriore procedura (cfr. n. 1.1).

Legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità

Il DFF ha sottoposto per consultazione all'IFPDT il progetto di legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità (LMeCA) in cui sono contenuti numerosi obiettivi nel campo della trasformazione digitale dell'Amministrazione federale. L'Incaricato si è espresso in merito e ha chiesto e ottenuto dall'Amministrazione che migliori e precisi vari aspetti.

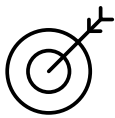
Con una legge trasversale come la LMeCA l'Amministrazione federale mira a raggiungere, nel quadro della trasformazione digitale e dell'ampliamento dei suoi servizi digitali, un utilizzo efficace e moderno dei dati che superi i confini delle unità amministrative. Nel progetto di legge vengono disciplinati diversi aspetti, come per esempio le basi per la pubblicazione dei dati dell'Amministrazione per il libero riutilizzo (open government data) e per la messa a disposizione e l'impiego dei mezzi delle tecnologie dell'informazione e della comunicazione da parte delle autorità federali oppure il principio dello scambio elettronico automatico dei dati mediante interfacce e l'esercizio di una piattaforma di interoperabilità.

L'IFPDT apprezza il mandato dell'Amministrazione federale per la trasformazione digitale e riconosce i vantaggi dell'interoperabilità digitale dei dati. Ricorda tuttavia ciclicamente anche che è necessario riconoscere e identificare per tempo i rischi che questi obiettivi comportano per i diritti delle persone interessate. Nel suo parere sulla LMeCA l'Incaricato ha quindi ripetutamente fatto riferimento alla necessità di realizzare una valutazione d'impatto dei rischi. Il progetto di legge, con le sue varie richieste, non traccia una distinzione sufficientemente chiara tra dati oggettivi e dati personali, il che comporta varie difficoltà per quanto riguarda una sua delimitazione dalla legge sulla protezione dei dati. L'IFPDT ha dunque chiesto precisazioni in diversi ambiti.

Nessun ampliamento degli accessi ai dati

In considerazione del principio *once only* e dell'utilizzo multiplo dei dati, nel progetto della LMeCA è stata istituita una base legale nella legge sulla statistica federale che consente all'Ufficio federale di statistica (UST) di accedere a dati già a disposizione di

autorità terze mediante una procedura di richiamo, sempre che altre leggi non prevedano altrimenti. L'IFPDT ha richiesto in questo contesto che l'accesso sia limitato ai dati di cui l'UST



necessita per i suoi compiti statistici e che dunque la nuova procedura non possa portare a un ampliamento dell'accesso ai dati. Ha

inoltre chiesto che il messaggio concernente la LMeCA menzioni esplicitamente che gli organi federali interessati devono escludere dall'accesso tutti i dati di cui l'UST non ha bisogno, soprattutto se si tratta di dati personali. Il Consiglio federale dovrà definire in dettaglio a livello di ordinanza quali organizzazioni sono tenute a mettere a disposizione dell'UST i dati nell'ambito della procedura di richiamo prevista, oltre che il tipo di dati e di settori tematici.

Per promuovere la trasformazione digitale dell'Amministrazione federale il progetto di legge contiene inoltre le basi per lo svolgimento di progetti pilota in particolare per le innovazioni tecniche. Al riguardo l'IFPDT ha sottolineato che i progetti pilota devono essere eseguiti in primo luogo in conformità all'articolo 35 della nuova

legge sulla protezione dei dati, sempreché siano soddisfatti i requisiti per l'applicazione della norma. Al di fuori del campo d'applicazione di quest'ultima i progetti pilota secondo la LMeCA possono essere autorizzati dal dipartimento competente dopo avere ottenuto il parere dell'IFPDT e di altri servizi specializzati. Il progetto di legge prevede inoltre che le persone interessate debbano essere previamente informate del trattamento dei dati previsto durante i progetti pilota e che possano dare il loro consenso, aspetti che l'Incaricato apprezza.

In seguito alla consultazione i servizi responsabili hanno preso in considerazione le nostre osservazioni e hanno già apportato le corrispondenti modifiche al progetto o hanno previsto di farlo. L'IFPDT continuerà a seguire l'attuazione dei singoli progetti.

L'IFPDT esprime critiche sulla rilevazione dei dati fiscali

L'Ufficio federale di statistica (UST) ha sottoposto all'IFPDT un progetto di modifica dell'ordinanza sulle rilevazioni statistiche il quale prevede una nuova rilevazione dei dati fiscali. In considerazione dei notevoli rischi dal profilo della protezione dei dati insiti nel progetto, l'IFPDT ha chiesto un'adeguata valutazione dei rischi.

Uno dei primi progetti nell'ambito del programma Gestione dei dati a livello nazionale (NaDB) è l'introduzione di una nuova rilevazione dei dati fiscali da parte della Confederazione: i dati amministrativi disponibili presso l'Amministrazione federale delle contribuzioni (AFC) e i dati fiscali disponibili presso le amministrazioni fiscali cantonali potranno così essere utilizzati per scopi di statistica federale (in applicazione del principio «once only», cfr. in merito anche il 28° Rapporto d'attività, n. 1.1).

In vista dell'attuazione concreta del progetto, nell'estate 2021 l'ufficio responsabile, ossia l'Ufficio federale di statistica (UST), ha sottoposto alle unità amministrative un progetto di modifica dell'allegato all'ordinanza sulle rilevazioni statistiche. Il progetto prevedeva tra l'altro una nuova rilevazione dei dati fiscali. In base a questa modifica i Cantoni avrebbero dovuto rilevare annualmente tutti i dati sull'imposta sul reddito e sulla sostanza per

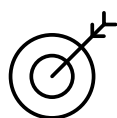
le persone fisiche e quelli sull'imposta sull'utile e sul capitale per le persone giuridiche. L'AFC è stata designata quale organo di rilevazione. I dati non resi anonimi avrebbero inoltre dovuto essere messi a disposizioni dell'AFC e dell'UST per scopi statistici.

Durante la consultazione degli uffici l'IFPDT ha criticato il modo in cui il progetto verrebbe concretizzato. Ha sottolineato che i dati fiscali consentono di avere un quadro completo di una persona, pertanto il progetto rappresenta un'ingerenza considerevole nella personalità degli interessati. In futuro verrebbero così trattati grandi quantità di dati nonché dati degni di particolare protezione come informazioni sulla religione, sulle malattie, sull'assistenza sociale ecc. di ogni singolo contribuente in Svizzera. La valutazione statistica dei dati per contribuente comporta anche il pericolo di profilazione e, di conseguenza, presenta un alto potenziale di rischio. Il fatto che l'AFC e l'UST possano valutare lo stesso set di dati per scopi statistici



diversi farebbe ulteriormente aumentare i rischi. In questo contesto l'IFPDT ha chiesto all'UST di effettuare previamente un'adeguata valutazione dei rischi, vale a dire di identificare e valutare i

rischi e definire le misure atte a contrastarli. L'IFPDT ha pure sottolineato che il principio della destinazione vincolata deve essere osservato soprattutto nei progetti che comportano un uti-



lizzo multiplo dei dati. Va dunque in ogni momento garantita, in particolare presso l'AFC, la separazione tecnica e organizzativa dei dati per scopi di vigilanza da quelli per scopi statistici. L'IFPDT si è infine anche chiesto se l'attuale base legale nel settore della statistica federale soddisfi ancora le esigenze del principio di legalità.

Dopo questa consultazione degli uffici l'UST e l'IFPDT hanno avuto un colloquio. Nel settembre 2021 l'UST ha poi informato l'IFPDT che il rilevamento dei dati fiscali non faceva più parte delle modifiche previste nell'allegato all'ordinanza sulle rilevazioni statistiche.

APP DI INCONTRI

Analisi del trattamento dei dati

L'IFPDT ha proseguito il suo accertamento dei fatti riguardante un'app svizzera d'incontri.

Nella primavera del 2021 l'IFPDT ha avviato un accertamento dei fatti presso il fornitore svizzero di un'app di incontri, dopo aver ricevuto comunicazione che gli utenti dell'app avevano difficoltà a richiedere la cancellazione del proprio conto. Oltre a chiarire questo punto, il nostro accertamento ha riguardato anche la trasmissione dei dati personali a terzi e il rispetto dei requisiti in materia di trasparenza e di sicurezza dei dati (cfr. 28° rapporto d'attività, n. 1.1).

Nell'anno in esame l'IFPDT ha stilato i fatti e li ha sottoposti al fornitore affinché si esprimesse in merito. I fatti sono stati in seguito chiariti con il fornitore e su questa base l'IFPDT sta effettuando l'analisi giuridica dei fatti accertati. Al momento della stesura del presente rapporto d'attività, questa procedura era ancora in corso.

Lavori in vista dell'entrata in vigore della LPD riveduta

REVISIONE OLPD

All'inizio del 2021 l'IFPDT ha pubblicato sul suo sito Internet una sintesi delle principali novità introdotte con la revisione del 25 settembre 2020 della legge sulla protezione dei dati. Secondo quanto annunciato dal DFGP, al Consiglio federale sarà proposto di porre in vigore questa legge non come inizialmente previsto nella seconda metà del 2022 ma soltanto il 1° settembre 2023.

Nell'estate 2021 l'Ufficio federale di giustizia (UFG) ha sottoposto all'IFPDT un primo progetto dell'ordinanza d'esecuzione relativa alla nuova LPD. Da allora l'IFPDT ha espresso le sue considerazioni in diversi pareri. Alla fine dell'anno in rassegna non erano ancora stati trattati tutti i punti che secondo l'IFPDT andavano migliorati.

Parallelamente a questa consulenza in merito al lavoro legislativo, l'IFPDT si sta occupando della realizzazione di tre portali digitali. Questi permetteranno di elaborare in modo efficiente le notifiche che la legge prevede per i consulenti aziendali per la protezione dei dati così come per i registri delle attività di trattamento e le violazioni della sicurezza dei dati. L'IFPDT sta inoltre rinnovando il suo sito Internet. (cfr. n. 3.2).

Nuova ordinanza relativa alla legge sulla protezione dei dati riveduta

Proseguono a pieno regime i lavori per la nuova ordinanza relativa alla legge sulla protezione dei dati riveduta.

L'IFPDT ha presentato le sue osservazioni all'Ufficio federale di giustizia, organo cui compete la revisione.

L'IFPDT ha ricevuto per la prima volta il progetto di ordinanza relativa alla legge sulla protezione dei dati riveduta nell'estate 2021 quando è stato invitato a partecipare alla consultazione. Da allora ha espresso il suo punto di vista in diversi pareri e discussioni e ha avuto colloqui con l'Ufficio federale di giustizia (UFG), organo cui compete la revisione, in merito alle disposizioni che ritiene vadano migliorate. Rimangono tuttavia ancora numerosi punti che, secondo l'IFPDT, necessitano di essere ulteriormente migliorati. Ritiene anche che le critiche espresse dai partecipanti alla consultazione pubblica siano per molti aspetti comprensibili e ha invitato l'UFG a tenerne conto nel proseguimento dei lavori relativi al progetto. Al termine della consultazione e dopo aver sentito l'Incaricato anche le Commissioni delle istituzioni politiche di entrambe le Camere hanno chiesto adeguamenti del progetto. Alla fine dell'anno in rassegna i lavori relativi alla revisione dell'OLPD erano ancora in corso.

Disposizioni in parte troppo poco dettagliate

Secondo l'IFPDT le disposizioni d'esecuzione relative alle valutazioni d'impatto sulla protezione dei dati, al profiling, alle decisioni individuali automatizzate e alle normative in materia di emolumenti sono ancora lacunose e poco dettagliate, il che rende difficile applicare la legge rispondendo al

criterio della certezza del diritto. In particolare il progetto attuale di ordinanza non contempla lo strumento centrale della valutazione d'impatto sulla protezione dei dati. Per esempio, non è ancora stato stabilito in quale momento gli organi federali devono presentare tale valutazione all'IFPDT. In questo contesto avremmo gradito che l'ordinanza prevedesse che i risultati delle valutazioni d'impatto sulla protezione dei dati e i pareri al riguardo espressi dall'Incaricato confluiscono nei rispettivi messaggi legislativi all'attenzione delle Camere federali.

Sebbene l'UFG preveda aiuti interpretativi informali, l'assenza di indicazioni più dettagliate da parte del legislatore fa sì che per l'adempimento dei loro obblighi di trattamento l'economia e gli organi federali dovranno basarsi in gran parte sul testo di legge. Inoltre, senza ulteriori precisazioni nell'ordinanza, l'IFPDT avrà, in qualità di autorità di vigilanza, un ampio margine di manovra nell'applicare le disposizioni di legge nell'intento di assicurare una prassi uniforme e l'eguaglianza di trattamento; se dovesse sfruttare appieno tale margine rischierebbe di essere accusato di agire come un regolamentatore.

L'IFPDT ha inoltre proposto di completare le disposizioni d'esecuzione sull'assistenza amministrativa, tanto più che nel suo parere del 9 novembre 2016 sulla mozione del

PLR «Evitare i doppioni nella protezione dei dati» (16.3752) il Consiglio federale aveva già rilevato la problematica della vigilanza parallela esercitata dalle autorità di protezione dei dati estere da un lato e dall'IFPDT dall'altro.

Rafforzare il ruolo dei consulenti per la protezione dei dati degli Uffici federali

Negli ultimi anni l'IFPDT ha attribuito sempre maggiore peso ai responsabili della protezione dei dati dei titolari privati del trattamento dei dati, considerandoli come interlocutori primari a monte dell'autorità di vigilanza sulla protezione dei dati per quanto riguarda i progetti di digitalizzazione del settore privato. Il legislatore ha anche riportato nella revisione della legge sulla protezione dei dati la crescente importanza della protezione dei dati a livello aziendale. Ciò che sta già dando buoni risultati nel settore privato, deve essere praticato sempre più anche nell'Amministrazione federale, se si vuole che l'IFPDT gestisca i suoi compiti legali con i mezzi a sua disposizione anche in base al nuovo diritto. In questo contesto l'IFPDT chiede che l'attuale progetto di ordinanza attribuisca maggiore importanza al ruolo dei consulenti per la protezione dei dati degli organi federali. In particolare riteniamo indispensabile che per i progetti legislativi dell'Amministrazione federale il Consiglio federale preveda un nuovo obbligo di consultare i consulenti per la protezione dei dati degli Uffici federali.

Wenn Kategorien deaktiviert sind, sind die zugeordneten
zugeordneten Cookies aus dem Browser entfernt und
jede zugeordnete Kategorie und zugeordnete Cookies

[Lernen Sie mehr](#)

ALLE COOKIES ERLAUBEN

ALLE ABWEHREN



Notwendige Cookies

Notwendige Cookies stellen die Kernfunktionen dar.
diese Cookies kann die Website nicht ohne Cookies
und können nicht deaktiviert werden.



Benutzereinstellungen

Cookies ermöglichen es uns darüber hinaus, Ihre
und unsere website den Anforderungen anzupassen.
Dies kann das Speichern ausgewählter Inhalte
beinhalten.

EINSTELLUNGEN SPEICHERN

Sviluppo di portali di notifica online

Per l'attuazione della nuova legge sulla protezione dei dati (LPD) l'IFPDT metterà a disposizione due nuovi portali di notifica online, collegati al suo sito Internet:

- il portale di notifica delle violazioni della sicurezza dei dati destinato ai titolari del trattamento dei dati per l'adempimento del loro obbligo di notifica di cui all'articolo 24 della nuova LPD. Il portale permetterà di fornire all'IFPDT le informazioni necessarie in modo sicuro e rapido;
- il portale di notifica dei consulenti per la protezione dei dati che consentirà ai titolari privati e agli organi federali di trasmettere in modo semplice le informazioni necessarie all'IFPDT. Secondo la nuova LPD, per i privati la nomina dei consulenti rimane facoltativa; solo gli organi federali saranno tenuti a farlo per legge.

L'attuale portale di notifica e ricerca di collezioni di dati, il cosiddetto «Webdatareg», sarà completamente rinnovato. Contrariamente ai titolari privati, anche in base alla nuova LPD gli organi federali dovranno notificare all'IFPDT i loro registri delle attività di trattamento (in precedenza collezioni di dati). L'IFPDT pubblica questi dati sul suo sito Internet.

Adeguamento dell'ordinanza sulle certificazioni in materia di protezione dei dati

Nell'ambito della revisione totale della legge federale sulla protezione dei dati (LPD), non è stata adeguata soltanto l'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD), bensì anche l'ordinanza sulle certificazioni in materia di protezione dei dati (OCPD). L'IFPDT ha seguito i lavori relativi al progetto di revisione dell'OCPD. D'ora in poi la certificazione dovrà comprendere anche i servizi.

Oltre ai sistemi di trattamento dei dati (procedure, organizzazione) e ai prodotti (programmi, sistemi), la revisione dell'ordinanza sulle certificazioni in materia di protezione dei dati (OCPD) prevede la possibilità di certificare anche determinati servizi. Questo consentirà, per esempio, di aumentare la trasparenza del trattamento dei dati o di ridurre il rischio di violazioni della protezione dei dati, in modo tale da migliorare la fiducia in un servizio. I titolari del trattamento oggetto di una certificazione sono svincolati dall'obbligo di procedere a una valutazione d'impatto sulla protezione dei dati. La certificazione comprende tutte le componenti del trattamento dei dati che avrebbero dovuto essere verificate tramite una valutazione d'impatto sulla protezione dei dati.



Nell'articolo 6 OCPD è ora menzionata la norma ISO 27701, che completa la norma ISO/IEC 27001 con la protezione dei dati e può essere applicata soltanto in combinazione con quest'ultima. La norma ISO/IEC 27001 disciplina i sistemi di gestione per la sicurezza delle informazioni. L'aggiunta delle componenti rilevanti per la protezione dei dati (ISO 27701) a questa norma è intesa a migliorare la protezione dei dati nelle offerte di servizi in tutto il mondo. La procedura di certificazione rimane facoltativa.

L'IFPDT segue i lavori relativi all'OCPD dal profilo giuridico e informatico/tecnico. Stiamo in contatto con l'Ufficio federale di giustizia (UFG) e con altri organi federali, quali il Servizio di accreditamento svizzero (SAS), nonché con altri servizi di certificazione privati.

Il progetto non era ancora stato completato al momento della stesura del presente rapporto. Le informazioni di cui sopra corrispondono alla situazione alla fine dell'anno in esame. L'FDPIC continua a sostenere i lavori.

IDENTITÀ ELETTRONICA

Chiesta una nuova soluzione statale

Respingendo la legge sull'Ie nel 2021 la popolazione svizzera ha fatto chiaramente capire di volere che l'identità elettronica sia di competenza esclusiva dello Stato. L'IFPDT si adopera affinché anche questa nuova soluzione sia realizzata nel rispetto della protezione dei dati: essa deve convincere la popolazione in termini di sicurezza tecnica, di facilità d'utilizzo e di possibilità di autodeterminazione.

Dopo che nella votazione del 7 marzo 2021 il Popolo ha respinto la legge sull'Ie, in Consiglio nazionale sono state presentate sei mozioni di ugual tenore con le quali tutti i gruppi parlamentari chiedono una nuova identità elettronica: l'identità elettronica deve essere uno strumento d'identificazione elettronica statale che consente di comprovare la propria identità (autenticazione) nel mondo virtuale; la procedura di rilascio e la gestione complessiva devono rimanere di competenza esclusiva delle autorità statali; nel realizzare l'identità elettronica vanno osservati

i principi della minimizzazione dei dati, della «privacy by design» e della registrazione decentralizzata dei dati.

Tre soluzioni

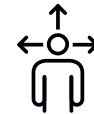
Le mozioni sono state accolte e il Consiglio federale ha quindi incaricato il DFGP (UFG e fedpol) di elaborare, assieme al DFF, alla Cancelleria federale, ai Cantoni e ai politecnici federali, un nuovo concetto d'identità elettronica che soddisfi queste richieste. Il DFGP ha progettato un concetto di base articolato su tre soluzioni per l'identità elettronica o meglio tre diversi livelli d'ambizione per quanto riguarda il sistema di identità elettronica:

- a) una soluzione Ie per mezzo di un fornitore d'identità centrale statale;
- b) una soluzione Ie mediante infrastruttura a chiave pubblica; e
- c) una soluzione Ie per mezzo della Self-Sovereign Identity.

La direzione del progetto ha tenuto informato l'IFPDT sugli sviluppi del progetto. L'UFG ha anche svolto una consultazione pubblica informale sul concetto di base.

Anonimato nello spazio pubblico

In questo contesto l'IFPDT è stato invitato a presentare le sue considerazioni sul documento di discussione degli obiettivi dell'Ie durante una conferenza pubblica. L'Incaricato ha sottolineato che, indipendentemente dalla soluzione scelta, occorre garantire che



l'identità elettronica non finisca per impedire ai cittadini di muoversi in modo anonimo nello spazio digitale. Ha anche auspicato che ai cittadini il cui terminale è parte integrante dell'infrastruttura sia dato il necessario supporto per ricercare soluzioni decentralizzate in modo da poter contribuire alla sicurezza del sistema senza l'imposizione di obblighi legali.

Ora che il Consiglio federale ha preso una decisione orientativa su come sarà configurata la nuova identità elettronica, il DFGP elabora un progetto di legge che sarà pronto entro metà 2022. L'IFPDT continuerà a esprimere le sue considerazioni durante tutto l'arco del progetto.

NUOVE REGOLE

Trasparenza del finanziamento della vita politica

In seguito a un'iniziativa popolare depositata nel 2017, nel 2021 il Parlamento ha modificato la legge sui diritti politici per inserirvi norme volte a garantire una certa trasparenza nel finanziamento della vita politica. L'IFPDT ha ora rivolto la sua attenzione all'ordinanza d'esecuzione, attualmente oggetto di una procedura di consultazione esterna. Nell'autunno 2017 è stata depositata un'iniziativa popolare intitolata «Per più trasparenza nel finanziamento della politica (Iniziativa sulla trasparenza)» e, nell'agosto 2018, il Consiglio federale ha proposto di respingerla. Nel 2019 la Commissione delle istituzioni politiche del Consiglio degli Stati ha redatto un rapporto ed elaborato un controprogetto all'iniziativa. Nel luglio 2021 l'Assemblea federale ha modificato la legge federale sui diritti politici

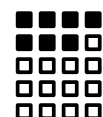
(LDP) e adottato norme volte a introdurre una certa trasparenza nel finanziamento della vita politica. I partiti politici saranno quindi tenuti a pubblicare dati, soprattutto quelli dei donatori, relativi ai doni importanti – il cui importo varia a seconda che si tratti di un'elezione o di una campagna di voto.

Il Controllo federale delle finanze (CDF), l'autorità incaricata di svolgere i compiti derivanti dalle modifiche della LDP, ha contattato l'IFPDT nell'ambito dei lavori relativi all'ordinanza di esecuzione, poiché sia la legge sia l'ordinanza contemplano la pubblicazione di dati di natura politica, ossia di dati potenzialmente sensibili se riconducibili a una persona specifica. In una riunione del settembre 2021, il CDF e l'IFPDT hanno potuto avere uno scambio di idee e chiarire numerosi punti.

Richieste dell'IFPDT

Nel novembre 2021 il progetto di ordinanza è stato posto in consultazione presso alcuni uffici federali. In questo contesto, l'IFPDT ha chiesto che nell'ordinanza fossero apportate alcune precisazioni supplementari allo scopo di

garantire la certezza del diritto e di meglio inquadrare il trattamento dei dati sensibili. Così, dato che il CDF deve pubblicare i dati nel modo in cui



li riceve dai movimenti politici, è stato precisato il concetto di documenti che dovranno essere pubblicati e di documenti

che servono per effettuare controlli. Si trattava di evitare la pubblicazione di dati personali dei donatori (per esempio il loro numero di conto bancario) che non servono ai fini della trasparenza del finanziamento della vita politica. È stata infine inserita nell'ordinanza una durata di cinque anni per la pubblicazione dei dati.

La procedura di consultazione esterna si è svolta dal 17 dicembre 2021 al 31 marzo 2022.

IC 8 12:16 **Romanshorn**
Winterthur Frauenfeld

FA	2	2	2	2	2	1	1	1	1	1
A	B	C	D							

ABG

 **SBB CFF FFS**

5 2

La Confederazione sviluppa una rete di know-how basata sull'AI

L'IFPDT è stato consultato dall'Ufficio federale dell'informatica (UFIT) in merito a un progetto pilota che intende realizzare una rete di know how basata sull'intelligenza artificiale (AI, Artificial Intelligence) all'interno dell'Amministrazione federale. Con l'acquisto di un simile prodotto sarà utilizzato un algoritmo che, sulla base di una valutazione digitale di dati seriali dell'Amministrazione federale, indirizzerà le tematiche internamente avvalendosi delle pertinenti conoscenze di esperti. In una prima fase l'UFIT eseguirà un'analisi d'impatto nell'ambito protezione dei dati.

Attualmente nell'Amministrazione federale sono impiegati i tradizionali motori di ricerca full-text. Questi non possono né operare autonomamente connessioni fra i risultati ottenuti né, di regola, fornire risultati riferiti a uno specifico contesto. Offrono unicamente

la possibilità di ricercare parole fornendo risultati per uno o più concetti di ricerca in un contesto ristretto (p. es. un servizio di SharePoint). Con questi strumenti tradizionali, la connessione fra potenziali vettori di conoscenze non può essere sostenuta in modo mirato.

A differenza delle attuali funzioni di ricerca o degli attuali elenchi di persone, la rete all'esame dell'UFIT, con il coinvolgimento di un'impresa privata, riconoscerà e riunirà il know how presente nell'Amministrazione federale e lo metterà a disposizione di tutti i collaboratori. Grazie ai principi dell'intelligenza artificiale, l'algoritmo collega le persone con know how affine per fornire una risposta rapida e qualificata a determinati quesiti e per sostenere la condivisione di esperienze all'interno dell'Amministrazione federale. A questo scopo l'algoritmo allestisce profili dettagliati di know how partendo da problematiche e risposte attinenti temi ben definiti già immesse nel sistema. Sulla base di questi profili un processo automatico indirizzerà le questioni ai collaboratori idonei. A problematiche a cui è già stata data una risposta l'algoritmo fornirà risposte automatiche,

che necessitano soltanto di un controllo da parte di vettori umani di conoscenze.

Nel settembre 2021, su richiesta dell'UFIT, l'IFPDT ha rilasciato una prima valutazione scritta delle condizioni quadro in materia di protezione dei dati per l'esecuzione di un primo progetto pilota. L'IFPDT aveva consigliato all'Ufficio di effettuare un'analisi d'impatto sotto il profilo della protezione dei dati con lo scopo di evidenziare i rischi potenziali del previsto tratta-



mento di dati personali e le misure per ridurli. Dai risultati dell'analisi eseguita nel febbraio 2022, nonché dagli accertamenti

effettuati parallelamente dall'UFIT in materia di protezione delle informazioni e diritto del personale, dipenderà il seguito dei lavori e il concetto per la messa in atto dell'esercizio pilota.

1.2 Giustizia, polizia, sicurezza

REVISIONE TOTALE DELLA LEGGE SULLE DOGANE

Istituzione dell'Ufficio federale della dogana e della sicurezza dei confini

L'IFPDT ha accompagnato i lavori legislativi dell'Ufficio federale della dogana e della sicurezza dei confini (UDSC) relativi alla legge sui compiti d'esecuzione dell'UDSC (LE-UDSC) e l'elaborazione parallela di una valutazione d'impatto sulla protezione dei dati dal profilo del diritto in materia di vigilanza. Nella terza consultazione degli Uffici, l'UDSC ha adottato fondamentali proposte di miglioramento formulate dall'IFPDT.

L'11 settembre 2020 il Consiglio federale ha aperto la consultazione su un pacchetto legislativo – con la denominazione abbreviata «Legge sui compiti d'esecuzione dell'UDSC» (LE-UDSC) – inteso a creare le basi legali per il programma di digitalizzazione e trasformazione (DaziT) dell'Amministrazione federale delle dogane (AFD), la quale dal 1° gennaio 2022 è stata rinominata in «Ufficio federale della dogana e della sicurezza dei confini» (UDSC).

L'IFPDT ha accompagnato la revisione legislativa e i lavori paralleli per la formulazione di una valutazione d'impatto sulla protezione dei dati dal profilo del diritto in materia di vigilanza. Su nostra richiesta, l'UDSC ha documentato in che misura il trattamento di dati personali secondo la nuova legislazione differisce, in termini di portata e intensità, da quello effettuato secondo il diritto anteriore. Abbiamo inoltre suggerito che, nella valutazione d'impatto sulla protezione dei dati, oltre ai rischi legati alla sicurezza l'UDSC illustri anche i rischi sistemici che derivano dalla fusione dei compiti delle ex unità dell'AFD Dogana e Corpo delle guardie di confine nella nuova categoria professionale «Specialista dogana e sicurezza dei confini», nonché la nuova struttura delle applicazioni sotto forma di un unico sistema informativo.

Dopo la conclusione della terza consultazione degli Uffici, l'IFPDT constata che il capitolo sul trattamento dei dati presenta notevoli miglioramenti (in merito alla prima consultazione degli Uffici cfr. 27° Rapporto d'attività, n. 2.4; in merito alla seconda consultazione cfr. 28° Rapporto d'attività, n. 1.2). L'UDSC ha accolto fondamentali suggerimenti di miglioramento dell'IFPDT anche nel completamento della valutazione d'impatto sulla protezione dei dati. Alla fine del periodo in rassegna non era ancora possibile stabilire definitivamente fino a che punto le divergenze residue potranno essere eliminate.



REVISIONE DELLA LEGGE SULLE ATTIVITÀ INFORMATIVE

La revisione deve garantire lo stesso livello di trasparenza della LAIn attuale

Nel novembre 2020 il Servizio delle attività informative della Confederazione (SIC) ha informato l'IFPDT di una revisione della legge federale sulle attività informative (LAIn) intesa in particolare ad aggiungervi nuovi compiti, un nuovo concetto di trattamento dei dati e ad adattarla alla nuova legge sulla protezione dei dati (LPD). La consultazione degli uffici nell'estate 2021 ha permesso di migliorare in modo considerevole il progetto e i requisiti dell'IFPDT sono stati rispettati. Persiste una divergenza relativa alla citazione del sistema d'informazione. La procedura di consultazione dovrebbe svolgersi nella primavera 2022.

Entrata in vigore il 1° settembre 2017 dopo una votazione indetta in seguito a un referendum, la legge federale del 25 settembre 2015 sulle attività informative (LAIn) deve ora essere sottoposta a una revisione totale volta in particolare a semplificare la gestione dei

dati in adempimento di un mandato conferito dalla Delegazione delle Commissioni della gestione delle Camere federali.

Il mandato ha portato a una revisione del capitolo sul trattamento dei dati, in cui è stato introdotto un cambiamento di paradigma che prevede di sostituire i molteplici sottosistemi d'informazione con un unico sistema.

Durante le diverse fasi della consultazione, l'IFPDT è riuscito a fare in modo che venissero accettati numerosi requisiti relativi alle disposizioni sul trattamento dei dati. Nel messaggio concernente la legge sarà pertanto espressamente stabilito che il futuro trattamento dei dati personali non dovrà essenzialmente differenziarsi dal trattamento previsto dal diritto vigente a livello di categorie di dati e di regole d'accesso. Nel progetto di legge queste categorie di dati sono state distinte in modo che – nonostante l'eliminazione dei sottosistemi – il trattamento dei dati possa sempre essere attribuito a compiti specifici del SIC.

Fino all'ultimo non è stato tuttavia possibile raggiungere un accordo su un punto essenziale, poiché il DDPS non si è lasciato convincere a inserire nel progetto di legge che in futuro il SIC deve per principio trattare tutti i dati

personali relativi all'attività informativa nel sistema unico sopraccitato. L'IFPDT ricorda che il trattamento da parte dell'ex polizia federale di informazioni riguardanti l'attività informativa in una moltitudine di ubicazioni poco trasparenti costituiva un importante punto critico sollevato dal rapporto della Commissione d'inchiesta parlamentare del 22 novembre 1989 sullo scandalo delle schedature.

Bisogna invece lodare la volontà espressa di avvicinare il diritto d'accesso previsto dalla LAIn a quello della nuova LPD, rafforzando quindi i diritti delle persone coinvolte.

È pure positiva la volontà di abbandonare l'idea, da noi criticata, di limitare ulteriormente la validità della legge federale sul principio di trasparenza dell'amministrazione (LTrans) mediante questa revisione.

La consultazione esterna dovrebbe iniziare nel secondo trimestre 2022.

DIRITTO D'ACCESSO

Richieste di verifica in caso di differimento

Nell'ambito del diritto d'accesso a certi dati personali trattati dal Servizio delle attività informative della Confederazione (SIC) e dall'Ufficio federale di polizia (fedpol), la comunicazione delle informazioni può essere differita senza indicarne i motivi. Il richiedente può tuttavia chiedere all'Incaricato di verificare se il trattamento dei dati è conforme al diritto e se il differimento è giustificato. Tra il 2018 e il 2021 l'IFPDT ha trattato 274 richieste di verifica.

Quando riceve una richiesta di verifica, l'Incaricato invia al richiedente una conferma di ricezione. Nel contempo informa l'ufficio responsabile del trattamento (SIC o fedpol) della richiesta di verifica. L'ufficio in questione indica in seguito all'IFPDT se il richiedente è registrato nei suoi sistemi d'informazione oppure no.

Il richiedente non è registrato

Se il richiedente non è registrato nei sistemi d'informazione, l'ufficio responsabile ne informa l'IFPDT mediante un «attestato di non registrazione». L'IFPDT esamina quindi la richiesta di verifica. Se il richiedente adduce in modo verosimile che il differimento della risposta lo lede in modo grave e irreparabile, l'Incaricato informa l'ufficio responsabile che intende pronunciare una raccomandazione (SIC) o una

decisione (fedpol), che lo invita a informare immediatamente il richiedente del fatto che non è registrato. L'ufficio ha quindi la possibilità di spiegare all'Incaricato in che modo una comunicazione dei dati alla persona in questione costituirebbe una minaccia per la sicurezza interna o esterna. Se questo non è il caso, l'ufficio informa il richiedente del fatto che non è registrato. L'IFPDT invia quindi la comunicazione prevista dalla legge. Questa comunicazione, dal tenore sempre identico, informa il richiedente che nessun dato che lo riguarda è stato trattato illegalmente oppure che l'Incaricato ha pronunciato una raccomandazione (SIC) o una decisione (fedpol) per rimediare a un errore relativo al trattamento dei dati o al differimento della risposta.

Il richiedente è registrato

Se il richiedente è registrato nei sistemi d'informazione, due collaboratori dell'Incaricato si recano nei locali dell'ufficio responsabile per verificare la liceità del trattamento dei dati registrati. In seguito a questa verifica, l'Incaricato esamina se il richiedente rende verosimile che un differimento della risposta lo lederebbe in modo grave e irreparabile. Se l'IFPDT giunge alla conclusione che un trattamento dei dati è contrario al diritto, che le condizioni per il differimento non sono soddisfatte o che le condizioni per un'informazione immediata sono riunite, informa l'ufficio della sua intenzione di pronunciare una raccomandazione (SIC) o una decisione (fedpol). L'ufficio ha quindi la possibilità di presentare le sue argomentazioni. Al termine della verifica l'IFPDT invia la comunicazione prevista dalla legge, esattamente identica a quella descritta per il caso in cui il richiedente non è registrato.

Qualche cifra

Negli ultimi quattro anni (2018 – 2021) l'IFPDT ha trattato 274 richieste di verifica.

Le richieste di verifica basate sulla legge sulle attività informative sono state le più numerose (180): 8 nel 2018, 42 nel 2019, 107 nel 2020 e 23 nel 2021. Le richieste basate sulla legge sui sistemi d'informazione di polizia della Confederazione sono state meno numerose (93): 29 nel 2018, 25 nel 2019, 17 nel 2020 e 22 nel 2021. Abbiamo ricevuto una sola domanda di verifica in applicazione della legge sull'assistenza internazionale in materia penale.

Attività di coordinamento a livello nazionale

Anche nell'anno in rassegna l'IFPDT era in contatto permanente con le autorità europee e i Cantoni per garantire un'applicazione uniforme delle disposizioni sulla protezione dei dati per quanto riguarda l'impiego delle diverse componenti del sistema d'informazione di Schengen.

Negli ultimi anni il gruppo di coordinamento di controllo del SIS II ha constatato nel sistema d'informazione Schengen (SIS) un aumento dei bandi di concorso per il controllo discreto e il controllo specifico di persone e veicoli nell'ambito della prevenzione delle minacce e della tutela della sicurezza interna ed esterna degli Stati Schengen (art. 36 della decisione UE SIS II 2007/533/GAI) (cfr. n. 1.8). Per questa ragione ha elaborato un questionario su questo tema che va compilato dalle diverse autorità di protezione dei dati

Schengen a livello nazionale. L'IFPDT ha in seguito verificato presso l'Ufficio federale di polizia (fedpol) la legittimità del trattamento dei dati, in particolare la loro cancellazione nel contesto summenzionato, e inviato il questionario compilato al segretario del gruppo di coordinamento di controllo del SIS II. Sulla base delle sue constatazioni



l'IFPDT è giunto alla conclusione che attualmente non è necessario intervenire a questo riguardo nei confronti di fedpol.

Nelle videoconferenze del 1° luglio 2021 e 2 dicembre 2021 l'IFPDT ha discusso con i rappresentanti delle autorità cantonali di protezione dei dati nel gruppo di coordinamento di controllo Schengen in merito agli sviluppi attuali in ambito Schengen. Nelle sedute si è parlato anche delle esperienze e constatazioni fatte sui controlli dei logfile.

In vista della valutazione Schengen della Svizzera pianificata per il 2023, l'8 novembre 2021 si è tenuta a Berna una seduta kick-off con le autorità coinvolte. Il coordinamento superiore della valutazione Schengen è assicurato

primariamente dalla direzione della delegazione svizzera nel comitato Schengen. Quest'ultima è composta dall'Ufficio federale di giustizia (UFG), cui compete la responsabilità primaria, e dalla divisione Europa della segreteria di Stato DFAE, che condivide la responsabilità. I lavori sono svolti in 9 sottogruppi di lavoro e l'IFPDT partecipa al sottogruppo protezione dei dati. Nel primo semestre 2022 i questionari dovranno essere recapitati alle autorità partecipanti. Trascorso un termine di risposta di otto settimane, le risposte pervenute saranno esaminate. All'inizio del 2023 è previsto un sopralluogo da parte degli esperti europei.



1.3 Commercio ed economia

VALUTA DIGITALE DIEM

Diem ritira in Svizzera il progetto per un sistema di pagamento tramite blockchain

Nella primavera 2021 la Diem Association (precedentemente Libra Association) ha ritirato la richiesta di autorizzazione presentata all'Autorità federale di vigilanza sui mercati finanziari (FINMA) per un sistema di pagamento tramite blockchain in Svizzera. L'IFPDT ha perciò concluso la sua attività di consulenza e vigilanza relativa a questo progetto iniziata nel 2019.

La Diem Association con sede a Ginevra (Diem) è un'organizzazione a carattere associativo che intendeva creare un sistema di pagamento tramite blockchain. L'IFPDT ha contattato Diem (a quel tempo ancora Libra Association) per la prima volta nel luglio 2019 dopo aver preso conoscenza del progetto. Da quel momento in poi ha intrattenuto contatti regolari con i responsabili di Diem e con rappresentanti di diversi organi di vigilanza nazionali e internazionali (cfr. 27° Rapporto d'attività, Tema prioritario II).

Nel corso della primavera 2021, su richiesta dell'IFPDT Diem ha presentato diversi documenti di rilievo dal profilo della protezione dei dati, in particolare una bozza del concetto di protezione dei dati e una della valutazione dell'impatto dei rischi. L'obiettivo dell'IFPDT

consisteva nel riuscire a formulare una valutazione del progetto dal punto di vista tecnico e della protezione dei dati sulla base delle informazioni ottenute.

Nel corso delle nostre analisi, nel maggio 2021 Diem ha annunciato il trasferimento strategico delle proprie attività principali dalla Svizzera agli Stati Uniti. In quel momento Diem progettava di lanciare il sistema di pagamento in una prima fase dagli Stati Uniti. Inoltre, per il momento dovevano venire collegati soltanto fornitori di servizi finanziari negli Stati Uniti.

Di conseguenza Diem ha deciso di ritirare la richiesta di autorizzazione per un sistema di pagamento in Svizzera presentata alla FINMA e oramai a buon punto. Di conseguenza l'IFPDT ha interrotto i suoi accertamenti. Secondo le informazioni dei media il progetto sta per scomparire anche negli Stati Uniti.

PROCEDURA DI VIGILANZA SEC

La trasmissione di dati all'autorità statunitense di vigilanza sulle borse è per principio ammissibile

Su richiesta dell'autorità statunitense di vigilanza sulle borse (United States Securities and Exchange Commission; SEC) l'IFPDT ha verificato se le imprese svizzere registrate presso la SEC possono fornire a quest'ultima dati richiesti dal diritto statunitense nell'ambito di una procedura di vigilanza della SEC senza violare la legislazione svizzera sulla protezione dei dati. La risposta fornita dall'IFPDT, che ha redatto a questo proposito un memorandum, è fondamentalmente affermativa. La questione della trasmissione di dati personali protetti dal diritto penale rimane aperta.

Nell'anno in esame l'autorità statunitense di vigilanza sulle borse (United States Securities and Exchange Commission; SEC) ha indirizzato uno scritto all'IFPDT invitandolo a verificare se le imprese svizzere registrate presso la SEC possono fornire a quest'ultima dati personali richiesti dal diritto statunitense nell'ambito di una procedura di vigilanza della SEC senza violare la legge federale sulla protezione dei dati (LPD). Finora la SEC non permetteva alle imprese svizzere di registrarsi poiché temeva di non ricevere i dati necessari in eventuali procedure di controllo.

Dopo aver ricevuto i documenti necessari l'IFPDT ha redatto un memorandum a questo proposito, giungendo alla seguente conclusione: in assenza di un livello di protezione dei dati adeguato negli Stati Uniti, le imprese

svizzere possono trasmettere dati personali alla SEC soltanto se è soddisfatto uno dei motivi che giustificano la comunicazione di dati all'estero secondo l'articolo 6 capoverso 2 LPD. Diversi di tali motivi sono applicabili alla trasmissione di dati alla SEC.

Innanzitutto, una comunicazione regolare di dati alla SEC è giustificata perché il trattamento è in relazione diretta con la conclusione o l'esecuzione di un contratto (art. 6 cpv. 2 lett. c LPD). Un possibile motivo giustificativo può tuttavia essere costituito anche da un interesse pubblico preponderante (art. 6 cpv. 2 lett. d LPD) o dal consenso della persona interessata (art. 6 cpv. 2 lett. b LPD).

L'IFPDT non ha espressamente precisato se e a quali condizioni è possibile comunicare alla SEC dati personali protetti non solo secondo la LPD, ma anche in virtù del diritto penale (ossia dati che sottostanno al segreto bancario). Non rientra nelle competenze dell'IFPDT interpretare il codice penale svizzero o eventuali altre leggi pertinenti. Il memorandum è pubblicato sul sito Internet dell'IFPDT. La SEC non ci ha fornito ulteriori dettagli in merito alle conclusioni tratte a proposito della possibilità, per le imprese svizzere, di registrarsi.

NEGOZI ONLINE

Trattamento di dati dei clienti

[Nell'ambito di un accertamento dei fatti, nell'anno in rassegna l'IFPDT ha chiarito alcune questioni e ambiguità riguardo alla valutazione dei dati dei clienti presso uno dei maggiori negozi online svizzeri.](#)

All'inizio del 2021 l'IFPDT ha avviato una procedura nei confronti di uno dei maggiori negozi online svizzeri, per controllare se il trattamento dei dati dei suoi clienti fosse conforme alla protezione dei dati. Il nostro accertamento ha riguardato tra l'altro il trattamento da parte del gerente del negozio online delle richieste di opposizione presentate dai clienti.

Dopo che in un accertamento preliminare abbiamo potuto constatare che il gerente respingeva le opposizioni contro determinati trattamenti dei dati, in particolare per quanto riguarda la registrazione e la valutazione del comportamento d'acquisto in forma personalizzata, il nostro accertamento si è concentrato sulla questione se simili trattamenti dei dati possano avvenire contro l'espressa volontà dei clienti (cfr. 28° Rapporto d'attività, n. 1.4).

Nell'anno in rassegna l'IFPDT ha analizzato il trattamento di dati in questione e interpellato il gerente. Il 26 gennaio 2022 ha quindi potuto accertare i fatti e, in base a essi, ha avviato una valutazione giuridica. Tale valutazione era ancora in corso al momento della stesura del presente rapporto.

SWISS MARKETPLACE GROUP

Piattaforma d'aste Ricardo: nuovi sviluppi nella procedura

[Anche nel corso dell'anno in rassegna ci sono stati nuovi, importanti sviluppi nella procedura avviata nel 2017 contro Ricardo e il TX Group in relazione all'utilizzo di dati raccolti sulla piattaforma d'aste online ricardo.ch.](#)

Dal 2017 abbiamo informato ogni anno sugli sviluppi della procedura di accertamento dei fatti avviata nei confronti di Ricardo e del TX Group. Secondo la nostra valutazione giuridica dei fatti, la profilazione, che il TX Group effettua ai fini di una pubblicità mirata sulla scorta di dati in provenienza da fonti diverse, deve essere chiaramente riconoscibile per gli interessati i quali, in questo caso, devono inoltre dare anche il loro esplicito consenso (cfr. n. 1.4 nel 28° Rapporto d'attività).

ESAME DELLA CAPACITÀ CREDITIZIA

Nel frattempo sulle piattaforme di Ricardo e del TX Group sono state apportati importanti adeguamenti e modifiche. In questo contesto abbiamo esaminato in particolare le nuove «Consent Management Platforms» (CMP). Abbiamo inoltre verificato il «legitimate interest assessment» presentatoci nell'agosto 2021, in cui il TX Group afferma di disporre di un interesse privato preponderante all'utilizzo dei dati di Ricardo e alla profilazione multiplatforma per la pubblicità mirata del gruppo, cosicché l'accordo degli interessati risulta superfluo.

A fine novembre 2021 il TX Group ci ha inoltre comunicato che l'11 novembre 2021 le aziende TX Group AG, Ringier AG, die Mobiliar AG e General Atlantic hanno fondato una joint venture comune con Swiss Marketplace Group (SMG). Sotto la SMG sono ora riuniti diversi mercati digitali, tra cui anche Ricardo AG con i suoi portali e le sue offerte. L'IFPDT sta ora verificando come queste modifiche tecniche e organizzative si ripercuotono sui trattamenti di dati rilevanti nella presente procedura. In chiusura di redazione del presente rapporto gli accertamenti erano ancora in corso.

Accertamenti presso una società di leasing per auto

L'IFPDT ha potuto concludere, senza adottare provvedimenti formali, gli accertamenti iniziati nello scorso anno in rassegna presso una grande società di leasing per auto riguardanti i trattamenti di dati relativi all'esame della capacità creditizia dei clienti. La società di leasing ha promesso di attuare due proposte di miglioramento dell'IFPDT concernenti il consenso.

Per poter stipulare un contratto di leasing per un'auto, i clienti devono acconsentire che la società di leasing verifichi la loro capacità creditizia. Da alcune richieste di cittadini l'IFPDT è venuto a conoscenza che una società di leasing richiede ai propri clienti il consenso per essere autorizzata a procurarsi numerose informazioni presso terzi per valutarne la capacità creditizia. I clienti interessati devono dare il loro consenso anche per l'ottenimento di informazioni su terze persone come coniugi o familiari.

Nel dicembre 2020 l'IFPDT ha pertanto avviato i primi accertamenti presso la società di leasing allo scopo di verificare se questi trattamenti di dati rimangano entro i limiti ammissibili dalla legge sulla protezione dei dati (cfr. 28° rapporto, n. 1.4). Dopo aver valutato il parere della società di leasing, l'IFPDT è giunto alla conclusione che i trattamenti di dati descritti destinati a esaminare la capacità creditizia e la

solvibilità di chi richiede un leasing sembrano ampiamente conformi alle prescrizioni previste dalla protezione dei dati.

L'IFPDT ha tuttavia formulato alcune riserve su un trattamento di dati riguardante i partner dei richiedenti che vivono nella stessa economia domestica.

Ha raccomandato alla società di leasing, nel caso in cui volesse giustificare il trattamento di dati dei partner con il loro consenso, di richiedere loro una firma autografa o una dichiarazione di consenso.

D'altro canto l'IFPDT ha contestato la presunta irrevocabilità della rimozione di blocchi di dati presso gli uffici d'esecuzione, la ZEK e l'IKO nonché la Posta svizzera. L'IFPDT ha reso attente le società di leasing che un consenso rilasciato in virtù della legislazione sulla protezione dei dati può essere revocato in ogni momento in modo informale e senza giustificazioni, ragione per cui qualsiasi clausola figurante nel modulo relativo al consenso secondo cui i blocchi di dati sono considerati «irrevocabilmente rimossi» va stralciata. La società di leasing ha promesso di attuare queste misure.





17:39

4G

Fabienne Muster

Heute

Hallo Fabienne 17:39 ✓

Wann bist du heute ca. vor Ort? 17:39 ✓

ca. 20.15 17:40

Ok, besten Dank 17:40 ✓

Ich warte beim Bahnhoftreffpunkt auf dich. 17:41 ✓

Super, freue mich, bis dann 👍 17:41

+

ja

aber

ich

q w e r t z u i o p ü
a s d f g h j k l ö ä
123

123



MITTO AG

Inchiesta su un possibile uso improprio dell'accesso al sistema di segnalazione SS7

In un rapporto pubblicato il 6 dicembre 2021 nei media sono state formulate gravi accuse contro un impiegato della Mitto AG, una società con sede a Zugo. Si dice che la Mitto invii SMS in tutto il mondo per varie grandi aziende consentendo così a terzi, dietro remunerazione, di effettuare una sorveglianza non autorizzata di individui.

Il «Bureau of Investigative Journalism», un'organizzazione non-profit di Londra, e Bloomberg News hanno pubblicato un rapporto secondo cui un dipendente della Mitto AG di Zugo avrebbe abusato dell'accesso concesso dagli operatori di telefonia mobile alle loro reti per l'invio di SMS, allo scopo di ottenere informazioni. Secondo il rapporto, avrebbe usato in particolare l'accesso al sistema di segnalazione (SS7) per consentire a terzi, dietro remunerazione, di effettuare una sorveglianza non autorizzata di individui.

Il 7 dicembre 2021 l'IFPDT ha aperto un'inchiesta preliminare. Come primo passo, ha chiesto alla Mitto AG di prendere una posizione e parallelamente ha contattato gli operatori di telefonia

mobile in Svizzera. Questi ultimi hanno confermato l'esistenza di una collaborazione con la Mitto AG, precisando tuttavia che vi sono sufficienti misure tecniche di protezione atte a impedire l'accesso illecito ai dati personali. Sulla base di questi primi riscontri, l'IFPDT non ravvisa per il momento indicazioni su eventuali abusi a danno della popolazione svizzera.

La Mitto AG ha comunicato all'IFPDT di non essere a conoscenza di un simile caso. L'azienda ha informato l'IFPDT, su sua richiesta, in merito alle misure tecniche e organizzative



implementate per proteggere i dati personali. Sulla base della documentazione ricevuta, l'IFPDT esaminerà se alla Mitto AG

si sono verificate inadempienze in relazione ai meccanismi di controllo e al rilascio di autorizzazioni ai collaboratori. In chiusura di redazione l'indagine era ancora in corso.

SOCIAL MEDIA

I nuovi termini di servizio di WhatsApp destano preoccupazioni in fatto di protezione dei dati

A gennaio 2021 il servizio di messaggistica istantanea WhatsApp ha reso nota un'imminente modifica dei suoi termini di servizio e dell'informativa sulla privacy. Nel contempo gli utenti venivano informati che era indispensabile approvare tali modifiche per continuare a utilizzare il servizio. L'IFPDT le ha esaminate e ha risposto alle domande dei cittadini e degli operatori dei media preoccupati.

Spesso si sostiene che la maggior parte delle persone sia disposta a dare via i propri dati senza esitare in cambio di un servizio gratuito. Le cose però sono andate diversamente quando WhatsApp ha annunciato i suoi nuovi termini di servizio. Incerti sul da farsi, alcuni cittadini hanno esposto le loro preoccupazioni all'IFPDT. Erano riluttanti



ad accettare le nuove condizioni perché temevano di perdere il controllo sui loro dati. Nel contempo si erano resi conto della loro

dipendenza dal servizio perché i loro familiari o amici non erano disposti a passare a servizi alternativi. L'IFPDT ha quindi analizzato in modo più approfondito le modifiche dei termini di servizio e dell'informativa sulla privacy.



È emerso che l'incertezza degli utenti era probabilmente dovuta all'esistenza di due diverse versioni dei termini di servizio e dell'informativa sulla privacy: una per la Regione europea (di cui fa parte anche la Svizzera) e una per gli altri Paesi del mondo. A quest'ultima sono state effettivamente apportate modifiche più estese. Il gruppo Meta (ex Facebook Inc.) ha ampliato per esempio il diritto di collegare tra loro in modo ancora più stretto i dati dei suoi diversi servizi (WhatsApp, Instagram e Facebook) e di utilizzarli anche a scopo di marketing o di condividerli con società terze. Questo non concerne il contenuto dei messaggi o delle chiamate, che rimane protetto dalla crittografia end-to-end e quindi inutilizzabile, ma soltanto i metadati. La raccolta e la valutazione di questi dati consente tuttavia a Meta di trarre diverse conclusioni sugli utenti: la frequenza con cui interagiscono con un gruppo o una persona, quali sono i loro interessi sulla base dei gruppi a cui appartengono ecc.

Quasi nessun cambiamento per gli utenti in Svizzera

Secondo gli accertamenti dell'IFPDT, per gli utenti che risiedono nella Regione europea (inclusa la Svizzera) il contenuto dei termini di servizio non è stato

pressoché modificato. I cambiamenti hanno perlopiù riguardato adeguamenti linguistici come precisazioni (p. es. informazioni sui metadati dei messaggi o sulla collaborazione con altre società del gruppo Meta) oppure aggiunte (p. es. per quanto riguarda la base giuridica del trattamento dei dati o del trattamento degli utenti che violano i termini di servizio e l'informativa sulla privacy o i dati conservati). Nuove sono soltanto le disposizioni che precisano quali dati potrebbero in futuro essere trattati se un privato contatta via WhatsApp una società utilizzando i nuovi account aziendali recentemente introdotti. Per chi non interagisce con gli account aziendali di WhatsApp, invece, non cambierà nulla. Questo è quanto ha comunicato ai cittadini e ai media L'IFPDT in risposta alle loro domande.

Anche se i timori degli utenti svizzeri si sono rivelati perlopiù infondati, le discussioni attorno alle nuove condizioni di WhatsApp hanno portato molti cittadini a riconsiderare l'uso dei servizi gratuiti. È così aumentata la consapevolezza che molte di queste offerte si basano su modelli aziendali incentrati sulla monetizzazione dei dati e che quindi vale la pena leggere più attentamente le condizioni generali e le dichiarazioni sulla protezione dei dati. È quanto suggeriamo di fare non soltanto quando si utilizzano servizi gratuiti ma sempre, indipendentemente dal modello di prezzo, quando si concludono contratti con fornitori di servizi, perché può accadere anche con i servizi a pagamento che i dati dei clienti vengano elaborati per scopi propri del fornitore di servizi.

L'IFPDT constata che, formulando le condizioni generali e l'informativa sulla privacy in modo dettagliato ma difficilmente comprensibile ai profani, la trasparenza supplementare è pressoché nulla. A questo proposito l'IFPDT si adopera per migliorare la qualità delle informazioni fornite agli utenti nell'ambito della sua attività di consulenza e di vigilanza.



ONELOG

Progetto degli editori di media svizzeri per un accesso comune a portali in rete

[Anche nell'anno in esame l'IFPDT si è informato presso le case editrici svizzere sui lavori inerenti al progetto per un accesso comune a portali in rete.](#)

I lavori delle case editrici svizzere per un accesso comune ai portali in rete che gestiscono (cfr. 28° Rapporto d'attività, n. 1.1.) sono proseguiti anche nell'anno in rassegna. Gli editori di media partecipanti hanno fondato la ditta OneLog, una joint venture che gestisce in modo centralizzato la soluzione Single-Sign-On (SSO) per lo più come responsabile del trattamento.

I miglioramenti proposti dall'IFPDT sono stati accolti e le pertinenti misure tecniche e organizzative implementate. È così escluso che gli editori di media scambino e colleghino dati personali tramite OneLog ottenendo in questo modo informazioni su utenti rilevate da altri editori di media.

OneLog ha anche elaborato processi e disciplinamenti pertinenti per assicurare che i dati continuino a essere protetti e consentire agli utenti di far valere i loro diritti (in particolare i diritti d'informazione, di cancellazione e di correzione). OneLog impegna per contratto anche gli editori di media partecipanti ad adempiere agli obblighi affinché utilizzino la soluzione SSO in modo rispettoso della protezione dei dati. OneLog ha inoltre designato un responsabile aziendale della protezione dei dati, il quale controlla che siano osservate in tutto il sistema le disposizioni pertinenti.

La soluzione SSO è stata lanciata nella tarda estate dell'anno in esame e da allora il login su diversi portali di media è effettuato attraverso OneLog. Non mancheremo di osservare le future fasi di sviluppo.

Completamento automatico dei dati del conto

Grazie alla segnalazione di un cittadino l'IFPDT è stato informato del fatto che nel sistema di e-banking di PostFinance si poteva accedere ai dati di un numero indefinito di titolari di conti postali. Nel frattempo, con l'ausilio di misure tecniche, la Posta ha limitato in modo proporzionato il completamento automatico dei dati del conto. L'IFPDT chiede inoltre che i clienti abbiano la possibilità di opporsi alla cosiddetta pubblicazione del conto.

Quando i signori Bernasconi effettuavano ancora la maggior parte dei loro pagamenti in contanti allo sportello postale, ci si assicurava manualmente che i dati dei beneficiari fossero corretti. Vi era un elenco accessibile al pubblico in cui erano riportati nomi e indirizzi di tutti i titolari dei conti postali. Alcuni anni fa questa cosiddetta pubblicazione del conto è stata trasferita nel sistema di e-banking di PostFinance: non appena viene inserito un numero di conto di PostFinance nell'apposito

campo riservato ai pagamenti, il sistema visualizza automaticamente il nome e l'indirizzo del titolare del conto. Questa funzione, limitata ai conti di PostFinance, riduce al minimo gli errori di digitazione e serve ancora oggi a garantire che il traffico dei pagamenti avvenga in modo sicuro e senza intoppi. I clienti di PostFinance vengono informati della pubblicazione del conto nelle Condizioni generali e in una scheda informativa separata.



In base a una segnalazione pervenutaci da un cittadino, nel sistema di e-banking di PostFinance era tuttavia possibile digitare un numero illimitato di numeri di conto. Questo significava che i numeri potevano essere provati a piacimento e che si potevano eseguire interrogazioni in blocco sui titolari dei conti. Su nostra richiesta PostFinance

VERIFICHE DELLA SOLVIBILITÀ

ci ha confermato che il limite di interrogazioni inizialmente implementato era stato inavvertitamente disattivato, per cui, per circa due anni, sono state possibili interrogazioni in blocco. Dopo che anche il cittadino si è rivolto direttamente a PostFinance, il limite di interrogazioni è stato nuovamente attivato, cosicché ora è possibile effettuare soltanto 10 interrogazioni ogni 24 ore.

L'IFPDT è giunto alla conclusione che lo scopo del completamento automatico dei dati dei titolari dei conti postali è comprensibile e che i clienti di PostFinance ne sono adeguatamente informati. Inoltre, il rischio di interrogazioni in blocco è stato ridotto a un livello accettabile grazie alla riattivazione dell'apposito limite.

Tuttavia, dato che la funzione non è obbligatoriamente necessaria per il traffico dei pagamenti e che, in ultima analisi, si basa sul consenso degli interessati, i clienti dovrebbero avere la possibilità di opporsi a tale uso dei loro dati. L'IFPDT ha quindi invitato PostFinance a introdurre un'opzione di opt-out.

Registrazioni errate nella banca dati di una società di riscossione

[Nell'ambito dell'accertamento in corso riguardante possibili registrazioni errate nella banca dati di una delle società più importanti nel settore della riscossione e della verifica della solvibilità, l'IFPDT ha acquisito informazioni supplementari fra l'altro sul tema della cosiddetta «famiglia di cattivi pagatori», ovvero dell'effetto negativo della cattiva solvibilità di un membro sull'economia domestica in cui vive.](#)

Come emerge dai nostri precedenti rapporti d'attività, nel febbraio 2020 l'IFPDT ha avviato una procedura d'accertamento dei fatti presso un grosso fornitore di servizi di riscossione e di verifica della solvibilità a causa di presunte registrazioni errate nella banca dati che hanno portato a confondere persone con nomi e indirizzi uguali o

simili e a causa delle difficoltà che sarebbero insorte nella correzione di tali registrazioni errate (cfr. 27° rapporto, n. 1.4).

In un secondo tempo, a seguito di richieste di cittadini e media, l'IFPDT ha esteso il campo d'indagine alla tematica della cosiddetta «famiglia di cattivi pagatori». Con questa espressione si fa riferimento alla situazione in cui, nell'ambito di una verifica di solvibilità, vengono divulgate informazioni sulla cattiva solvibilità di altre persone della stessa economia domestica (cfr. 28° rapporto, n. 1.4). La comunicazione di questa informazione a commercianti online è volta a impedire che persone con una cattiva solvibilità possano effettuare un acquisto contro fattura a nome di un membro della stessa economia domestica con una buona solvibilità (operazione di aggiramento).

La prassi di considerare la solvibilità di una famiglia nel suo insieme solleva interrogativi in materia di protezione dei dati, ragione per cui l'IFPDT ha



chiesto informazioni più precise all'impresa. La valutazione dal profilo giuridico di queste informazioni è ancora in corso.

L'IFPDT stabilirà il seguito della procedura sulla base dei risultati di questa valutazione.

ASSOCIAZIONI

Nuova tessera di membro con funzione di carta di credito integrata per i tiratori

La Federazione sportiva svizzera di tiro (FST) ha inviato a oltre 50 000 tiratori con licenza una nuova tessera di membro con funzione di carta di credito. Numerosi membri della Federazione hanno espresso il loro disappunto per tale impiego commerciale dei loro dati. L'IFPDT ha convenuto, nell'ambito di colloqui con la FST, un trattamento dei dati personali dei membri della Federazione conforme alla protezione dei dati.

L'invio di oltre 50 000 nuove tessere di membro con funzione di pagamento integrata ha suscitato in numerosi membri della Federazione interrogativi legati alla protezione dei loro dati. L'IFPDT ha dapprima chiesto alla Federazione informazioni supplementari in merito a questo impiego dei dati.

Già in passato la Federazione si era rivolta a una società esterna per l'emissione delle tessere di membro. Tuttavia, il nuovo fornitore di carte di credito

scelto persegue anche scopi propri e ottiene l'accesso a nuovi clienti. Nel caso della trasmissione di dati dei membri al fornitore della carta di credito si tratta dunque di una comunicazione di dati il cui trattamento deve rispettare i principi della legge sulla protezione dei dati, in particolare le finalità vincolate e la trasparenza.

I dati personali possono essere trattati soltanto per lo scopo indicato all'atto della loro raccolta, risultante dalle circostanze o previsto da una legge. Per quanto concerne le finalità vincolate, dal 2016 gli statuti della FST prevedono la comunicazione dei dati dei propri membri a fini commerciali contro la quale è però data la possibilità di opporsi. La FST ha quindi creato le basi necessarie per l'impiego commerciale dei dati dei suoi membri.

Si rivela tuttavia problematico il fatto che tali disposizioni siano contenute espressamente soltanto negli statuti della FST. Gli statuti delle 36 associazioni affiliate alla federazione e quelli di oltre 2000 società non includono, nella gran parte dei casi, regole analoghe ma si limitano a rinviare in maniera generale agli statuti della FST. Risultava quindi molto difficile per i singoli membri delle associazioni prendere atto di tali informazioni e, se del caso, opporvisi. L'IFPDT ha stabilito che la comunicazione dei dati da parte della FST al fornitore di carte di credito non è avvenuta in osservanza del principio di trasparenza sancito dalla legge sulla

protezione dei dati, in base al quale le finalità del trattamento devono essere riconoscibili da parte della persona interessata.

D'intesa con la FST è stato convenuto che sul suo sito Internet, nella sua rivista e mediante l'invio di una news-



letter essa informerà nuovamente i tiratori sulla comunicazione dei loro dati a fini commerciali e gli stessi potranno quindi

far valere il loro diritto di opposizione mediante una semplice comunicazione alla Federazione.

La FST deve quindi assicurarsi che il fornitore di carte di credito tratti separatamente i dati di coloro che desiderano avere unicamente una tessera di membro senza funzione di carta di credito e che non utilizzi tali dati per fini propri (p. es. marketing o promozioni). I membri che vogliono rinunciare completamente alla tessera di membro nel formato carta di credito potranno continuare a partecipare agli eventi indicando il loro numero di membro e presentando un normale documento d'identità.

1.4 Salute

CORONA

Accompagnamento del progetto per un certificato COVID-19 conforme alla protezione dei dati e per il certificato «light»

L'IFPDT ha preso parte in veste di consulente alle sedute del gruppo di progetto istituito dall'Ufficio federale della sanità pubblica per lo sviluppo di un certificato COVID-19 uniforme, a prova di falsificazione e riconosciuto a livello internazionale. In tale contesto ha insistito per l'istituzione di un certificato «light» con dati minimi.

Per far fronte alla pandemia di COVID-19, all'inizio della primavera 2021 la Svizzera ha introdotto il certificato COVID-19 per attestare l'avvenuta vaccinazione contro il COVID-19, la guarigione dall'infezione o il risultato negativo di un test eseguito di recente. La base per questo certificato figurava nell'articolo 6^a della legge COVID-19. Nell'ambito del suo obbligo legale di consulenza l'IFPDT si è adoperato nel gruppo di progetto istituito dall'Ufficio federale della sanità pubblica (UFSP) per garantire un'attuazione del mandato legale conforme alla protezione dei dati. Secondo quest'ultimo, un simile certificato doveva essere personale, a prova di falsificazione, verificabile nel rispetto delle norme sulla protezione dei dati e strutturato in modo da permettere una verifica decentralizzata o locale della sua autenticità e validità. Il certificato doveva quindi

poter essere utilizzato possibilmente per entrare e uscire da altri Paesi. L'IFPDT ha inoltre chiesto sin dall'inizio che l'introduzione del certificato non comportasse l'obbligo generalizzato di avere con sé uno smartphone. Si è tenuto conto di questa richiesta permettendo di utilizzare il certificato COVID-19 in forma sia digitale sia cartacea.

Certificato light con dati ridotti

L'IFPDT ha insistito e ottenuto che l'Ufficio federale dell'informatica e delle telecomunicazioni (UFIT) sviluppasse, oltre al certificato compatibile con l'UE destinato ai viaggi internazionali, un secondo certificato con codice QR per uso nazionale interno, il cosiddetto «certificato light». Quest'ultimo può essere generato nell'applicazione e non contiene informazioni da cui si deduce se il certificato sia stato rilasciato sulla base di un test, di una vaccinazione o della guarigione. Affinché non sia possibile risalire al motivo del

rilascio, il certificato light ha soltanto una breve durata di validità, dopodiché deve essere nuovamente generato. Vale unicamente in Svizzera.

Nel certificato light figurano dunque solo le indicazioni necessarie all'identificazione e una firma elettronica. In tal modo non vi è il rischio che, utilizzando un'applicazione di verifica diversa da quella messa a disposizione dalla Confederazione, vengano letti dal certificato illecitamente dati sanitari. Pertanto non è di regola necessario che, al momento del controllo all'entrata di una manifestazione, venga divulgata l'informazione sul modo in cui il visitatore ha ottenuto il certificato, se in seguito alla vaccinazione, alla guarigione o a un test.

Problematica del 2G

Nel dicembre 2021 l'evoluzione della pandemia ha indotto il Consiglio federale a limitare l'accesso a determinati luoghi e manifestazioni a persone con un certificato di vaccinazione o guarigione. Da quel momento il risultato negativo di un test non bastava quindi più quale condizione per l'entrata. Con questo disciplinamento denominato «2G» o «2G+» il certificato light non era più utilizzabile, perché, proprio per



13:31



COVID-ZERTIFIKAT



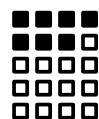
Nur mit einem Identifikationsdokument gültig

come era stato concepito, non forniva indicazioni sullo stato della persona (vaccinata, guarita o testata negativa). Questa restrizione non era stata prevista o non era prevedibile al momento dello sviluppo del sistema del certificato. Per poter utilizzare il certificato light anche con il 2G o con disciplinamenti validi parallelamente e diversificati in funzione della situazione, si dovrebbero generare diversi certificati light (2G+, 2G e 3G) o poter memorizzare le informazioni sul tipo di autorizzazione direttamente nel certificato light. Quest'ultima soluzione comporterebbe l'inserimento nel certificato light di un dato sanitario, ciò che contraddice il suo scopo originale. Indipendentemente dalla soluzione poi attuata, l'IFPDT ha chiesto che, in caso di ritorno al disciplinamento 3G, il certificato light possa essere nuovamente utilizzato sfruttando appieno le sue funzionalità.

Utilizzazione proporzionata del certificato

Oltre a intervenire sulla conformità del certificato alla protezione dei dati e sul suo sviluppo ulteriore dal profilo tecnico, l'IFPDT si è anche adoperato affinché l'utilizzazione del certificato non sia lasciata alla discrezione dei privati, bensì siano create condizioni quadro di diritto pubblico.

I requisiti per l'utilizzazione del certificato sono stati disciplinati nell'ordinanza sui provvedimenti per combattere l'epidemia di COVID-19 nella situazione particolare (ordinanza COVID-19 situazione particolare; RS 818.101.26). L'obbligo del certificato era stato previsto in un primo tempo solo per i grandi eventi; successivamente, vista l'evoluzione della pandemia, è stato esteso in diverse tappe a ulteriori settori, come ristoranti e bar, e istituzioni per il tempo libero, come musei, biblioteche, zoo, centri fitness, piscine



o casinò. Nell'ambito di diverse consultazioni degli uffici, sovente a brevissimo termine, l'IFPDT ha ripetutamente precisato che le restrizioni d'accesso sulla base di un certificato e il relativo trattamento di dati sullo stato di salute potevano

essere considerati proporzionati dal profilo del diritto sulla protezione dei dati soltanto se necessari e idonei per lottare contro la COVID-19 in ottica epidemiologica. Provare questa necessità spetta all'UFSP quale ufficio specializzato competente, le cui constatazioni e valutazioni hanno sempre rappresentato il riferimento per la linea di condotta dell'IFPDT.

In particolare, in relazione al possibile ampliamento dell'obbligo del certificato nel mondo del lavoro, l'IFPDT ha precisato che i datori di lavoro possono richiedere la presentazione di un certificato nell'ambito del loro obbligo di prevenzione soltanto dopo un'accurata ponderazione degli interessi ed esclusivamente in relazione a un insieme di misure di protezione concrete o all'attuazione di un programma di test.

CONTACTTRACING

Accertamento dei fatti concernente l'applicazione SocialPass

Nell'ambito di un accertamento dei fatti l'IFPDT ha esaminato l'applicazione privata «SocialPass», utilizzata per raccogliere i dati di contatto nei ristoranti e in occasione di eventi. Nel suo rapporto finale l'IFPDT ha raccomandato in particolare ai gestori di migliorare la sicurezza tecnica dell'applicazione e di limitare proporzionalmente le possibilità concesse alle autorità sanitarie cantonali di consultare i dati raccolti in modo centralizzato. Dopo averle inizialmente contestate, i gestori hanno accettato le principali raccomandazioni dell'IFPDT, applicandole in ampia misura.

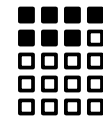
Quale misura di lotta contro la pandemia, i ristoratori e gli organizzatori di eventi sono stati obbligati, nell'estate del 2020, a raccogliere i dati di contatto dei loro ospiti per poterli trasmettere alle autorità sanitarie cantonali allo scopo di rintracciare i contatti (il cosiddetto «contact tracing») in caso di un'infezione da COVID-19 segnalata successivamente.

L'applicazione «SocialPass», gestita congiuntamente da due società private con sede in Svizzera, ha permesso una raccolta semplice di questi dati tramite smartphone. Tuttavia, diverse segnalazioni provenienti dalla popolazione hanno sollevato dubbi sulla conformità dell'app con la protezione dei dati inducendo l'IFPDT ad aprire, nel dicembre 2020, una procedura formale intesa ad approfondire anche le criticità emerse nelle notizie diffuse dai media. Nel suo rapporto finale l'IFPDT ha evidenziato numerose carenze che hanno dato luogo a dieci raccomandazioni, che i gestori dell'applicazione hanno in gran parte accettato dopo diverse videoconferenze cui hanno partecipato, tra l'altro, le autorità sanitarie dei Cantoni di Vaud e del Vallese.

Raccomandazioni principali dell'IFPDT e loro applicazione

Oltre ad avere constatato carenze di natura tecnico-organizzativa, l'accertamento dei fatti ha soprattutto permesso di appurare che i gestori privati dell'applicazione accordavano alle autorità sanitarie vodesi e vallesane un accesso diretto alla banca dati centralizzata rendendola disponibile per ricerche personali mirate di vario genere, nonostante l'assenza di motivi che giustificassero tale atto, in violazione

anche del principio di proporzionalità. Secondo le notizie diffuse dai media, nel Cantone del Vallese le possibilità di



consultazione accordate avrebbero condotto a trattamenti impropri di dati personali. Su raccomandazione dell'IFPDT i gestori

hanno infine riconosciuto le carenze inizialmente contestate e, stando alle loro dichiarazioni, le avrebbero eliminate.

Una procedura eccezionalmente lunga e complessa

L'applicazione privata SocialPass, utilizzata in tutta la Svizzera, elabora dati personali allo scopo di lottare contro la pandemia. In tale contesto l'IFPDT ha sempre dovuto tenere presente l'evoluzione epidemiologica per portare a termine tempestivamente l'accertamento dei fatti. Tuttavia, la procedura si è rivelata eccezionalmente lunga e complessa. Quando si è trattato di fissare i termini entro cui inviare le risposte, di evadere le numerose richieste di proroga e persino di ricusazione dei collaboratori dell'IFPDT

LEMIEVACCINAZIONI.CH

incaricati dei dossier, l'Incaricato ha dovuto tenere conto del fatto che verso l'inizio dell'estate 2021 la seconda ondata della pandemia si era ridotta. A quel punto la riapertura dei ristoranti era imminente e, di conseguenza, anche il riutilizzo dell'app SocialPass.

Per i motivi suesposti, nella citata procedura l'IFPDT doveva assicurarsi di informare in tempo utile la popolazione sulle possibilità tecniche di SocialPass e sui rischi per la protezione dei dati collegati alla sua utilizzazione. Il 31 maggio 2021 – giorno di riapertura dei locali interni dei ristoranti – l'Incaricato ha pertanto informato, mediante un comunicato stampa, sugli aspetti più importanti concernenti l'accertamento dei fatti e sui fatti constatati fino a quel momento, comprese le raccomandazioni principali.

L'accertamento dei fatti concernente SocialPass si è dimostrato necessario e utile, avendo offerto all'IFPDT l'opportunità di pronunciarsi sulle questioni di delimitazione delle competenze in materia di vigilanza tra Confederazione e Cantoni nonché su altre questioni inerenti al diritto di protezione dei dati che, per la loro importanza fondamentale, possono essere attribuite parzialmente anche ad altre applicazioni utilizzate da privati e autorità ai fini del tracciamento dei contatti.

Inchiesta concernente la piattaforma di certificati di vaccinazione

In seguito alle rivelazioni emerse nel marzo 2021 da una ricerca della rivista online «Republik», che denunciava gravi carenze dal profilo della protezione dei dati della piattaforma lemievaccinazioni.ch, l'Incaricato federale per la protezione dei dati ha aperto un procedimento formale contro il gestore della stessa. Le carenze riscontrate hanno reso impossibile l'ulteriore gestione della piattaforma e la fondazione, parzialmente finanziata dall'UFSP, ha infine dichiarato il fallimento. L'IFPDT ha sostenuto l'UFSP allo scopo di consentire agli interessati di accedere nuovamente ai propri dati.

Nella primavera del 2021, una ricerca della rivista online «Republik» ha rivelato che la piattaforma «lemievaccinazioni.ch» presentava gravi carenze dal

profilo della protezione dei dati e della sicurezza. La Fondazione mievaccinazioni, incaricata della sua gestione, era finanziata anche dall'Ufficio federale della sanità pubblica (UFSP), il quale promuoveva pure la piattaforma sul suo sito Internet e mediante opuscoli come «libretto di vaccinazione elettronico».

Dopo una valutazione sommaria sulla plausibilità delle accuse formulate l'IFPDT ha aperto una procedura di accertamento dei fatti in merito alla piattaforma sulla quale gli utenti documentavano le proprie vaccinazioni. Un audit successivamente avviato dalla Fondazione ha mostrato che le carenze rivelate dalla rivista online non potevano essere facilmente corrette, per cui la Fondazione ha messo per ora la piattaforma offline.

A fine luglio 2021 l'IFPDT ha presentato alla Fondazione il suo rapporto finale, mediante il quale formulava tre raccomandazioni riguardanti nello specifico l'integrità presumibilmente compromessa dei dati e la loro sorte in



caso di chiusura della piattaforma. In particolare, la Fondazione non poteva escludere che in passato si fossero già verificati

accessi non autorizzati e che i dati potessero essere stati alterati.

La Fondazione ha accettato le raccomandazioni dell'IFPDT e, poco dopo la conclusione dell'accertamento dei fatti, ha annunciato che avrebbe definitivamente cessato le sue attività operative e chiesto la liquidazione. Da quel

momento in poi, la Fondazione non ha più trattato le richieste di informazione e di cancellazione degli utenti. L'IFPDT ha quindi ricevuto regolarmente richieste da parte delle numerose persone interessate.

Nell'intento di rendere i dati accessibili agli interessati nonostante l'interruzione della piattaforma e l'imminente liquidazione dell'operatore, l'IFPDT ha fornito consulenza all'UFSP durante diverse riunioni svoltesi nel quadro del progetto di salvataggio dei dati «Datenrettung meineimpfungen», precisando le esigenze in ambito di protezione dei dati per l'invio agli utenti dei dati concernenti le vaccinazioni. Considerata la limitata disponibilità finanziaria e le carenze riscontrate nell'ambito dell'accertamento dei fatti, è risultato chiaro che, al fine di giungere a una soluzione pragmatica realizzabile in tempi brevi, occorreva accettare determinati compromessi in materia di protezione dei dati.

Nel novembre 2021 la Fondazione ha iniziato a inviare per e-mail agli utenti i loro dati di vaccinazione non criptati senza preannunciarlo. Diversamente da quanto dichiarato pubblicamente, questa procedura non è stata concordata con l'IFPDT ed era in contraddizione con le raccomandazioni emanate dall'Incaricato della protezione dei dati nel suo rapporto finale del 31 agosto 2021 nonché con le esigenze di un invio conforme alle disposizioni

in materia di protezione dei dati comunicate all'UFSP. In seguito all'intervento dell'Incaricato, la Fondazione ha sospeso gli invii. Poco dopo è stata aperta la rispettiva procedura di fallimento. L'IFPDT sta valutando la presentazione di una denuncia penale. Nell'anno in esame, gli accertamenti pertinenti erano ancora in corso.

L'IFPDT ha ora fatto pressione sull'UFSP affinché si assumi la propria responsabilità nonostante la procedura di fallimento in corso e continui a impegnarsi per una soluzione conforme alla protezione dei dati, al fine di mettere a disposizione degli utenti i loro dati di vaccinazione nel modo più conforme possibile alla protezione dei dati.

CARTELLA DEL PAZIENTE

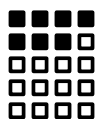
Consultazione, conservazione e cancellazione dei dati dei pazienti

[Un argomento ricorrente nell'attività di consulenza dell'IFPDT è la gestione delle cartelle dei pazienti, in particolare l'aspetto delle modalità e della tempistica con cui i pazienti possono esigere la propria cartella clinica o la cancellazione della stessa, nonché del periodo di tempo durante il quale i medici devono e possono conservare le cartelle. Una recente modifica del diritto in materia di prescrizione si ripercuote inoltre sull'aspetto della conservazione delle cartelle cliniche.](#)

Le domande ricorrenti rivolte all'IFPDT evidenziano anche nell'ultimo anno in esame un grande interesse, come pure alcune incertezze, in merito alla gestione delle cartelle cliniche. Una cartella del paziente, spesso definita anche cartella clinica, include dati che vengono registrati nel contesto di un trattamento medico, quali rapporti, radiografie, risultati di laboratorio e corrispondenza con altri fornitori di prestazioni mediche. Sulla base del diritto di accedere ai dati che li concernono, garantito dalla legge sulla protezione dei dati, i pazienti possono consultare la propria cartella clinica. Questo diritto è regolarmente esercitato nella pratica.

Per contro il diritto alla cancellazione dei propri dati, pure previsto dalla legge sulla protezione dei dati, entra in conflitto con gli obblighi di documentazione imposti ai professionisti medici dalle leggi sanitarie cantonali. Generalmente, infatti, un medico non può soddisfare la richiesta di un paziente di cancellare tutti i dati che lo concernono o di consegnargli tutti i documenti originali, poiché così facendo violerebbe il proprio obbligo legale di conservare i dati.

La legge sulla protezione dei dati fornisce soltanto una risposta indiretta alla domanda riguardante il periodo in cui un medico è tenuto e autorizzato a conservare le cartelle cliniche dei suoi pazienti. In base al principio di pro-



porzionalità, un medico può conservare le cartelle dei pazienti fintantoché i documenti corrispondenti sono necessari. Per esem-

pio, i documenti possono essere richiesti a scopo probatorio ben oltre la data di conclusione di un trattamento, ossia finché il termine di prescrizione per far valere eventuali rivendicazioni legate al trattamento corrispondente è scaduto o si può prevedere che ne deriverà una procedura giudiziaria. Di regola, si applicano dunque i termini di prescrizione generali del Codice delle obbligazioni.

Il 1° gennaio 2020 è entrato in vigore un adeguamento di tali disposizioni: il termine di prescrizione per i danni alle persone è raddoppiato (da 10

a 20 anni). Alcune leggi sanitarie cantonali che disciplinano gli obblighi di documentazione dei medici sono già state adeguate di conseguenza e prevedono ora a loro volta un obbligo di conservazione più esteso, andando a ripercuotersi sul periodo di conservazione delle cartelle dei pazienti. Si può dunque partire dal presupposto che il termine di prescrizione sia di 20 anni.

In caso di trattamento in ospedali con mandato di prestazioni cantonale si applica di regola il diritto cantonale e gli obblighi di conservazione e i termini applicati nel Cantone in questione.

Cartella informatizzata del paziente secondo LCIP

Sebbene le cartelle cliniche siano gestite sempre più digitalmente, di regola non si tratta (ancora) di cartelle informatizzate dei pazienti nel senso della legge federale sulla cartella informatizzata del paziente (LCIP). L'introduzione di questa forma di documentazione riferita al paziente continua tuttora a subire grossi ritardi – in parte dovuti alla pandemia. Nell'anno in esame, tuttavia, sono state certificate ulteriori comunità di riferimento, cui i fornitori di prestazioni – medici, terapisti, ospedali – possono aderire per poter offrire la cartella informatizzata ai propri pazienti. Dal maggio 2021 è stato infine possibile aprire le prime cartelle.

Parallelamente all'introduzione, è stata avanzata da più parti – in particolare dal mondo politico – la richiesta di adeguamenti della CIP al fine di promuoverne ulteriormente la diffusione. L'IFPDT segue le proposte e gli sviluppi pertinenti e si tiene regolarmente in contatto con l'UFSP, i Cantoni e altri attori.

SICUREZZA DEI REGISTRI

Vulnerabilità dei registri di donazione di organi e delle protesi mammarie

La protezione dei dati nell'ambito della consultazione dei registri nel settore sanitario non sembra essere sufficientemente presa in considerazione. Nel primo trimestre 2022 l'IFPDT è intervenuto in diversi casi problematici venuti alla ribalta delle cronache.

Dall'inizio del 2022 i media hanno attirato l'attenzione in particolare su due registri che presentano lacune rilevanti dal punto di vista della protezione dei dati.

Nel primo caso, concernente il registro nazionale di donazione di organi creato e gestito dalla fondazione Swisstransplant, il problema riguardava essenzialmente l'esattezza dei dati



inseriti. Era in effetti possibile iscrivere nel registro una terza persona – e quindi registrare la «sua» dichiarazione pro o contro

la donazione di organi – senza che questa fosse a conoscenza dell'iniziativa. Dopo aver verificato l'attendibilità dei fatti segnalatigli e preso le prime misure per limitare i danni, l'IFPDT ha avviato una procedura di accertamento dei fatti (art. 29 LPD), in occasione della quale i processi di identificazione saranno valutati e migliorati.

Il caso presenta anche una componente politica in considerazione della votazione del 15 maggio 2022. Il Popolo dovrà pronunciarsi su un cambio di sistema concernente la donazione di organi; attualmente occorre un consenso esplicito per poter effettuare un prelievo. Con la modifica proposta accadrà il contrario: in mancanza di

opposizione il prelievo sarà autorizzato (consenso presunto). La modifica sarà accompagnata dalla creazione di un nuovo registro in cui si potrà iscrivere la propria decisione in proposito; va osservato che si tratta di un registro diverso da quello qui in questione, anche se la sua finalità è simile.

Il secondo caso riguardava il registro delle protesi mammarie gestito da Swiss Plastic Surgery. Detto registro presentava lacune informatiche ed errori di progettazione che consentivano a persone non autorizzate di effettuare una consultazione ampia – e relativamente agevole – dei dati dei pazienti. Anche in questo caso l'Incaricato ha verificato l'attendibilità dei fatti denunciati e adottato misure intese a ridurre i danni. Il seguito della procedura è attualmente oggetto di valutazione da parte dell'IFPDT.

In generale, questi due casi recenti e l'affare della Fondazione mievaccinazioni (cfr. 28° Rapporto d'attività, n. 1.5) dimostrano che la sicurezza dei registri gestiti da associazioni private e da fondazioni, che trattano a volte anche dati personali su mandato delle autorità sanitarie, viene spesso trascurata. L'IFPDT insiste sul fatto che la



creazione di un registro implica che i suoi gestori siano pienamente consapevoli della loro responsabilità per quanto riguarda sia la sicurezza dei dati sia la loro esattezza. È perciò indispensabile disporre di un concetto completo di gestione

dei dati, dalla loro raccolta alla loro distruzione. Il tutto presuppone un'organizzazione IT, ma anche un'organizzazione del personale e una gestione degli accessi adeguate. Senza poi dimenticare l'informazione delle persone i cui dati vengono raccolti: in assenza di giustificativi, di cui il responsabile del registro potrebbe avvalersi, dette persone devono conoscere appieno l'impiego previsto dei loro dati prima di acconsentirvi.

ATTACCHI INFORMATICI

Dossier dei pazienti pubblicati nel darknet

Nel marzo 2022 i media della Svizzera francese hanno riferito che una grande quantità di dati relativi alla salute era stata pubblicata nel darknet. L'IFPDT ha chiesto che gli studi medici colpiti dai pirati informatici informino i pazienti in modo esauriente sull'incidente. Gli studi medici avevano già avviate le prime misure per contrastare eventuali lacune in materia di protezione e sicurezza dei dati. L'attacco è l'ennesima dimostrazione che in Svizzera i dati sanitari – degni di particolare protezione – spesso non sono sufficientemente protetti. L'IFPDT spera che i medici e i rappresentanti del ramo riconoscano l'urgenza di agire.

1.5 Lavoro

PERSONALE FEDERALE

Accertamenti presso l'Ufficio federale di statistica riguardanti la conservazione in forma cartacea dei dossier personali

L'IFPDT ha svolto accertamenti presso l'Ufficio federale di statistica (UST) riguardo alla gestione dei dossier personali in forma cartacea di ex collaboratori della Confederazione. È emerso che occorre intervenire. L'UST lo ha riconosciuto e ha sottoposto all'IFPDT una proposta concreta per ripristinare la legalità.

Il diritto in materia di personale federale prevede che i dossier personali siano conservati per dieci anni dopo la cessazione del rapporto di lavoro. Allo scadere del termine di conservazione, i dati sono offerti all'Archivio federale,

che distrugge quelli considerati senza valore archivistico. Un cittadino ha reso attento l'IFPDT che presso l'UST veniva conservato un ingente numero di dossier personali di ex collaboratori probabilmente oltre la durata di conservazione legale. L'IFPDT ha quindi avviato accertamenti preliminari presso l'UST.

È emerso che la conservazione dei dossier personali in forma cartacea di ex collaboratori non è conforme alle prescrizioni legali. Questi dossier personali non venivano distrutti dopo dieci anni, bensì conservati più a lungo. L'UST ha riconosciuto che occorre intervenire e, su richiesta dell'IFPDT, ha presentato un piano concreto di attuazione con le varie tempistiche allo scopo di ripristinare la legalità. I lavori necessari a questo scopo dovrebbero concludersi entro l'estate 2022. Alla luce di queste considerazioni l'IFPDT ha potuto rinunciare a una procedura formale di sorveglianza conformemente all'articolo 27 LPD.

1.6 Assicurazioni

VIGILANZA NELL'AMBITO DELL'ASSICURAZIONE MALATTIE

Chiarimento dei ruoli e delle competenze tra l'UFSP e l'IFPDT

L'IFPDT e l'Ufficio della sanità pubblica hanno intrapreso passi per chiarire i rispettivi ruoli e intensificare i contatti, dopo che il Controllo federale delle finanze ha constatato sovrapposizioni di competenze nell'attuazione della vigilanza sugli assicuratori malattie.

Gli assicuratori malattie sono tenuti a rispettare nella loro attività le disposizioni in materia di diritto delle assicurazioni sociali e protezione dei dati. Sottostanno in tal modo alla vigilanza sia dell'Ufficio federale della sanità pubblica (UFSP) sia dell'IFPDT. Nel rapporto del 21 maggio 2021 relativo a una verifica svolta presso l'UFSP sulla vigilanza nel settore delle assicurazioni, il Controllo federale delle finanze (CDF) ha constatato che occorre chiarire i ruoli dell'IFPDT e dell'UFSP e

disciplinare gli scambi e il coordinamento fra le due autorità (Audit CDF-20424).

Definire i ruoli e le norme per la segnalazione

Nella sua valutazione il CDF ha affermato che occorre mantenere o persino rafforzare l'efficacia della vigilanza dell'IFPDT e dell'UFSP sugli assicuratori malattie. La vigilanza sugli assicuratori malattie deve avvalersi dell'esperienza e della prossimità dell'UFSP, che svolge controlli sul posto, nonché delle competenze legali dell'IFPDT, le quali vengono ulteriormente rafforzate con la revisione totale della legge federale sulla protezione dei dati. Il CDF ha pertanto raccomandato all'UFSP di definire, in collaborazione con l'IFPDT, i ruoli e le regole per l'informazione reciproca fra gli assicuratori malattie e gli organi di vigilanza sui casi non conformi. Dal rapporto del CDF emerge anche che, in una perizia, l'Ufficio federale di giustizia (UFG) ha precisato le competenze dell'IFPDT e dell'UFSP nell'attuazione dei requisiti in materia di protezione dei dati stabilendo che la competenza spetta in linea di principio all'IFPDT. L'UFSP ha pertanto deciso di adeguare di conseguenza la sua Circolare 7.1 del 17 dicembre 2015 relativa

all'organizzazione e ai processi degli assicuratori malattie conformi alla protezione dei dati.

Chiarire le responsabilità

Nel suo parere sul rapporto di verifica del CDF, alla luce delle sovrapposizioni di competenze l'IFPDT valuta positivamente il coordinamento delle attività di vigilanza dell'UFSP e dell'IFPDT nell'ambito dell'assicurazione malattie come pure il chiarimento dei rispettivi ruoli e delle rispettive responsabilità. L'IFPDT ha tuttavia fatto notare che gli sforzi di coordinamento nel settore dell'assicurazione malattie non devono pregiudicare la sua indipendenza e che continuerà a esercitare la sua funzione legale di vigilanza nei confronti dell'UFSP.

Rafforzare gli scambi

Come raccomandato dal CDF nel suo rapporto di verifica, l'IFPDT ha partecipato all'elaborazione della circolare 7.1 dell'UFSP. Ha presentato diverse proposte d'integrazione, in particolare al fine di meglio coordinare le competenze. Nella bozza della circolare si è pertanto precisato che, nei limiti delle rispettive competenze, l'UFSP e l'IFPDT intratterranno uno scambio regolare, anche puntuale, se dovesse essere necessario coordinarsi in un caso specifico o ai fini di un'efficace vigilanza. È stato anche stabilito che le due autorità di vigilanza collaboreranno sostenendosi reciprocamente con le loro conoscenze specialistiche nei rispettivi campi dell'assicurazione malattie e della protezione dei dati. Inoltre gli assicuratori malattie sono stati resi attenti al fatto che lo stralcio di alcuni capitoli nella nuova circolare non significa che gli assicuratori siano svincolati dalle prescrizioni legali figuranti in quei capitoli. Per quanto riguarda la competenza dell'IFPDT nel valutare la conformità alla protezione dei dati e nel verificare dal profilo materiale i regolamenti sui trattamenti è stato precisato che

l'IFPDT agisce in qualità di autorità di vigilanza indipendente e tenuto conto delle sue risorse e priorità. La nuova versione della circolare 7.1 è stata inviata dall'UFSP a tutti gli assicuratori malattie nel dicembre 2021 ed è in vigore dal 1° gennaio 2022.

A margine delle discussioni sulla revisione della circolare, l'UFSP e l'IFPDT si sono accordate per designare le persone di contatto. Si incontreranno in futuro ogni anno per uno scambio e organizzeranno sedute ad hoc, come raccomandato dal CDF, allo scopo di rafforzare l'efficacia della loro vigilanza.

1.7 Trasporti

AUTOPOSTALE E FFS

Lacune nella sicurezza dei portali clienti

[Nell'anno in rassegna, la mancanza di sufficienti misure di sicurezza nei loro sistemi informatici ha reso possibile la fuga di dati dal portale clienti «ticketcontrol.ch» di Autopostale e dalla piattaforma «Nova» delle FFS. L'IFPDT ha chiesto ai consulenti per la protezione dei dati delle imprese interessate di dimostrare di aver preso le misure immediate necessarie per rimediare alle vulnerabilità e per informare i clienti.](#)

Nell'ambito di una ricerca, un gruppo di giornalisti è riuscito a visualizzare e copiare dati dal portale clienti «ticketcontrol.ch» senza troppe difficoltà. Dopodiché ha segnalato la fuga di dati ad Autopostale SA, che gestisce il portale, e si è messo in contatto con noi. L'IFPDT ha immediatamente invitato l'impresa responsabile a prendere posizione. Autopostale ha risposto prontamente, confermando l'accaduto. Analizzando i file di log degli accessi è stato



possibile tracciare l'attacco con facilità e attribuirlo a specifici aggressori. Nell'ambito di ulteriori indagini, Autopostale ha

potuto dimostrare all'IFPDT di aver eliminato la vulnerabilità del portale clienti subito dopo esserne venuta a conoscenza e che i set di dati ottenuti sono stati cancellati nel corso della ricerca.

Un'altra vulnerabilità è stata segnalata all'IFPDT per quanto concerne la piattaforma centrale di distribuzione NOVA, gestita dalle FFS per conto

dell'organizzazione settoriale dei trasporti pubblici Alliance SwissPass. In tale contesto, in un breve lasso di tempo un esperto in indagini informatiche è stato in grado di ottenere complessivamente un milione di set di dati contenenti dati su biglietti e abbonamenti. Dopo averci confermato la fuga di dati e aver rimediato immediatamente alla vulnerabilità, le FFS hanno inoltre informato l'IFPDT che anche le altre imprese di trasporto interessate hanno attuato le necessarie misure immediate e che i clienti non hanno subito alcun danno. L'esperto informatico ha quindi cancellato i dati scaricati.

In entrambi i casi i consulenti per la protezione dei dati delle imprese interessate hanno confermato che, grazie alle misure adottate, non sussistono più rischi sistemici sproporzionati sulle piattaforme in questione e che le persone interessate sono state informate in modo adeguato. Secondo l'IFPDT, il numero crescente di attacchi mirati ai sistemi informatici dimostra che i gestori devono in generale investire più risorse nella sicurezza informatica. Per i sistemi che presentano un rischio accresciuto per le persone interessate occorrerebbe inoltre effettuare regolarmente audit esterni.

DATI PNR

Consultazione degli uffici relativa alla nuova legge sui dati dei passeggeri aerei

[Il DFGP ha elaborato un progetto legislativo affinché i dati dei passeggeri rilevati dalle compagnie aeree possano essere utilizzati nella lotta al terrorismo e alla criminalità in Svizzera. L'IFPDT ha espresso il suo parere nell'ambito della consultazione degli uffici.](#)

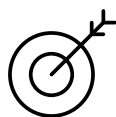
Al momento di prenotare un volo occorre fornire numerose informazioni alle compagnie aeree o alle agenzie di viaggio. Le autorità di sicurezza e di polizia auspicano che tali informazioni possano essere utilizzate per contrastare reati terroristici e forme gravi di criminalità. Diversi Stati europei hanno già designato unità (le cosiddette Passenger Information Units, PIU) incaricate di raccogliere, registrare e trattare i dati dei passeggeri. Per esempio, i dati devono poter essere confrontati con quelli delle banche dati delle autorità di perseguimento penale al fine di identificare le persone che potrebbero essere coinvolte in un reato terroristico o legato alla criminalità grave.

Il 12 febbraio 2020 il Consiglio federale ha deciso che anche la Svizzera deve avere la possibilità di utilizzare i dati dei passeggeri aerei. A metà 2021 il DFGP, in collaborazione con il DATEC, ha dunque elaborato un avamprogetto di legge sulla raccolta e il trattamento di dati dei passeggeri aerei da parte della Svizzera da porre in consultazione nonché la loro comunicazione a Paesi nei quali la protezione e il trattamento dei dati corrispondono allo standard richiesto nella direttiva UE 2016/681,

del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi (direttiva PNR UE).

Richiesto un elenco dei reati

Nel suo parere su un primo progetto, l'IFPDT ha rilevato l'importanza di rispettare i principi della legislazione sulla protezione dei dati nelle singole disposizioni, chiedendo in particolare che il margine di manovra delle Passenger Information Units (PIU) sia definito chiaramente e che al Servizio delle attività informative della Confederazione sia concesso solo un accesso limitato al sistema d'informazione PNR. Inoltre un elenco dei reati esaustivo



dovrà indicare a quale scopo i dati possono essere raccolti. L'IFPDT ha inoltre sottolineato che dovrà essere garantita la proporzionalità. Per esempio, occorre giustificare perché è necessaria una durata di conservazione di cinque anni per raggiungere lo scopo perseguito (cfr. 28° rapporto d'attività, n. 1.8.).

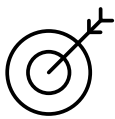


Parchimetri digitali con inserimento del numero di targa

Nell'anno in esame l'IFPDT ha ricevuto domande concernenti i parchimetri digitali con inserimento del numero di targa. A questo proposito ha espresso un parere in merito ai parcheggi gestiti da privati.

In ragione delle molteplici domande di cittadini, nell'anno in esame l'IFPDT ha osservato un aumento dei parchimetri digitali. Le persone interessate hanno espresso le proprie preoccupazioni circa la correttezza, dal profilo della protezione dei dati, della registrazione con il numero di targa.

Nel caso dei parcheggi che prevedono l'inserimento del numero di



targa, i numeri possono essere raccolti e utilizzati per effettuare la registrazione. Tuttavia i dati possono essere conservati

solo per il tempo strettamente necessario allo scopo perseguito. In base al

principio della trasparenza secondo la legislazione sulla protezione dei dati il responsabile del trattamento dei dati deve informare le persone interessate in modo appropriato sullo scopo della raccolta dei dati e sul periodo di trattamento e di conservazione corrispondente, se questi non risultano già chiaramente dalle circostanze.

Abbiamo segnalato alle persone interessate che, secondo l'articolo 8 della legge federale sulla protezione dei dati (LPD; RS 235.1), è possibile chiedere al detentore di una collezione di dati se e a quale scopo dati che le concernono sono trattati. Sul sito Internet dell'IFPDT sono reperibili i modelli di lettere corrispondenti.

Consultazione degli uffici relativa alla revisione parziale della legge sulla circolazione stradale

Nell'anno in esame la legge sulla circolazione stradale ha subito alcune modifiche. La legge disciplina ora anche la guida autonoma in Svizzera. L'IFPDT ha seguito il progetto e ha espresso il suo parere nell'ambito della consultazione degli uffici, chiedendo che le spiegazioni relative alla legge chiariscano le questioni legate alla proporzionalità, in particolare per quanto attiene alla durata della conservazione dei dati e alla loro cancellazione.

Con la revisione della legge sulla circolazione stradale (LCStr), sotto la direzione dell'Ufficio federale delle strade (USTRA), si intende permettere la guida autonoma in Svizzera. Il Consiglio federale dovrà poter stabilire in che misura i conducenti saranno dispensati dai loro obblighi e a quali condizioni potranno essere immatricolati veicoli autonomi privi di guidatore. Il progetto di revisione prevede che tali veicoli potranno circolare su singoli tratti predefiniti e sotto sorveglianza.

I veicoli a guida autonoma devono essere dotati di un registratore di modalità di guida che non può essere disattivato e che registra alcuni eventi relativi al sistema di automazione. Per esempio, viene memorizzato il momento del passaggio del controllo del veicolo dal conducente al sistema (o viceversa). Allo stesso modo viene registrato quando il sistema chiede al conducente di assumere il controllo. Il sistema registra automaticamente anche eventuali guasti tecnici.

DATI SULLA MOBILITÀ IN RETE

Secondo l'IFPDT le informazioni memorizzate nel registratore di modalità di guida possono essere collegate ai dati personali, per esempio del detentore del veicolo, senza particolari difficoltà. Abbiamo quindi accolto con favore il fatto che venga memorizzata la timbratura, ma non i dati relativi alla localizzazione. Ci siamo inoltre adoperati affinché la LCStr e le relative spiegazioni indichino inequivocabilmente chi può avere accesso ai dati del registratore di modalità di guida e per quali scopi chiaramente definiti, come pure se e quando tali dati possono essere valutati in riferimento a una persona. Tra le altre cose, questo ha lo scopo di evitare che i dati vengano utilizzati arbitrariamente.

L'IFPDT ha quindi sollevato questioni legate alla proporzionalità, per esempio in merito al termine di cancellazione, che dura fino al raggiungimento della capacità di memorizzazione e che pertanto può variare in funzione dell'uso del veicolo. Ha chiesto che le spiegazioni pertinenti siano completate. Anche per quanto riguarda la cancellazione dei dati dopo che il veicolo è stato ritirato dalla circolazione, l'IFPDT ha chiesto che le spiegazioni corrispondenti forniscano una motivazione.

Nella redazione del progetto l'U-STRa ha tenuto conto dei suggerimenti dell'IFPDT. Il 17 novembre 2021 il Consiglio federale ha presentato al Parlamento il messaggio concernente la modifica della legge federale sulla circolazione stradale.

Per lo scambio di dati sulla mobilità è necessaria una base legale

La Confederazione intende promuovere una mobilità efficiente che comprenda tutti i tipi di trasporto, anche facendo in modo che i diversi vettori possano più facilmente essere combinati fra loro. Ciò presuppone anzitutto che i dati e i servizi relativi alle diverse offerte di mobilità siano resi accessibili e disponibili agli utenti interessati. Nell'ambito della consultazione degli uffici, l'IFPDT ha preso posizione in merito al relativo progetto di legge.

La legge federale sull'infrastruttura di dati sulla mobilità (LIDMo) istituisce la base legale che permetterà di realizzare gradualmente un'infrastruttura nazionale di dati sulla mobilità (NADIM) preposta al loro scambio. Il compito di gestire la NADIM sarà affidato a un nuovo ente dei dati sulla mobilità (EDM). Le imprese private, come quelle degli sviluppatori di app e dei gestori di piattaforme, avranno in tal modo la possibilità di presentare ai loro clienti offerte interconnesse.

Ai sensi del progetto di legge, per dati sulla mobilità si intendono in primo luogo i dati tecnici come le informazioni riguardanti un sistema di trasporto, gli orari, le tariffe o altre informazioni analoghe. A seconda del tipo di offerta, per le operazioni di prenotazione e di pagamento, possono essere

richiesti anche i dati personali dei clienti. A talune condizioni, in questa categoria possono rientrare anche profili sugli spostamenti oppure – nel caso di offerte specifiche di viaggio per le persone a mobilità ridotta – dati personali degni di particolare protezione, che saranno trattati dall'EDM. Maggiori dettagli in proposito, fa sapere l'Ufficio federale dei trasporti (UFT), non sono per il momento disponibili; verranno definiti nel corso dell'ulteriore sviluppo del progetto.

L'IFPDT ha chiesto anzitutto che sia istituita la necessaria base legale per le categorie di dati che verranno trattati dall'EDM. Ha poi reso attenti sulla necessità che l'allestimento di una valutazione d'impatto sulla protezione dei dati, previsto nell'articolo 22 nLPD,

venga esaminato per tempo. Un tale esame permetterà di stabilire quali rischi comporta il trattamento di dati personali – risultanti dallo scopo dello stesso trattamento, dal contenuto o dal modo, dalla portata o dalla sua durata – per la sfera privata e l'autodeterminazione informativa delle persone interessate.

Come detto, l'elaborazione concreta dei dati, così come altri importanti aspetti riguardanti l'attuazione, verranno definiti nel corso dell'ulteriore sviluppo del progetto; per questa ragione l'IFPDT sarà in grado di esprimersi sul progetto nel suo complesso soltanto una volta che disporrà di tutte le informazioni necessarie.





1.8 Internazionale

Anche nel passato anno di attività la cooperazione internazionale è stata caratterizzata dalla crisi dovuta alla COVID-19. Praticamente, a causa della pandemia tutte le conferenze e sedute internazionali hanno dovuto svolgersi per videoconferenza. La 43^a Conferenza internazionale degli incaricati della protezione dei dati, che avrebbe dovuto tenersi nell'ottobre 2021 in Messico, è stata pianificata dapprima in forma ibrida, ma è stata poi svolta solo in remoto. Nel 2021, dopo aver posticipato una prima volta la data, si è infine rinunciato del tutto alla Conferenza europea delle autorità di protezione dei dati personali, prevista con cadenza annuale. L'FDPIC ha anche partecipato a vari eventi virtuali all'interno dell'OCSE quest'anno, per esempio sui temi «Data Governance and Privacy Challenges in the Fight against COVID-19» e «Data Localisation and Trusted Government Access to Data».

Gli incontri internazionali per videoconferenza non permettono purtroppo di intrattenere colloqui informali e allacciare relazioni personali dirette. In compenso, visto il risparmio in termini di tempo e costi dovuto ai mancati spostamenti, rispetto al solito ha potuto partecipare alle videoconferenze un numero maggiore di autorità di protezione dei dati e di loro collaboratori.

L'importanza della dimensione internazionale della protezione dei dati è emersa anche nel passato anno di attività. In seguito all'attività internazionale di molte imprese, si sono presentati problemi delicati inerenti alla protezione dei dati, segnatamente nell'ambito della trasmissione internazionale di dati personali, sia direttamente sia mediante memorizzazione nei cloud e su server all'estero.

Per questa ragione l'IFPDT è sempre presente a livello internazionale e partecipa attivamente negli organismi internazionali. Fra questi vi sono in particolare il Consiglio d'Europa, la Conferenza europea e la Conferenza internazionale delle autorità di protezione dei dati personali, l'Associazione francofona delle Autorità di protezione dei dati, l'OCSE nonché la cooperazione e il coordinamento internazionali delle autorità di protezione dei dati personali degli Stati Schengen e gli scambi con il Comitato europeo per la protezione dei dati (EDPB).

CONSIGLIO D'EUROPA

Protezione della vita privata dei bambini nell'ambiente digitale e linee guida relative alla profilazione e nell'ambito di campagne politiche

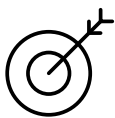
[Il Comitato consultivo della Convenzione 108 si è occupato, in occasione delle sue cinque riunioni, in particolare della preparazione di due documenti adottati dal Comitato dei Ministri nel 2021, vale a dire la dichiarazione sulla protezione del diritto dei bambini alla vita privata nell'ambiente digitale e l'adeguamento della raccomandazione del Comitato ministeriale concernente la profilazione. Il Comitato ha inoltre adottato linee guida relative alla protezione delle persone fisiche nel trattamento di dati personali nell'ambito di campagne politiche.](#)

Come nell'anno precedente, anche nel 2021 le riunioni del Comitato consultivo della Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale (Convenzione 108) si sono svolte in videoconferenza a causa della pandemia. Anche le sedute del rispettivo ufficio, di cui fa parte una rappresentante dell'IFPDT, si sono tenute virtualmente. Il Comitato si è occupato di questioni relative alla legislazione sulla protezione dei dati in merito a vari argomenti importanti e,

nella stessa occasione, ha adottato il suo programma di lavoro per gli anni dal 2022 al 2025. Il Comitato ha espresso il proprio parere sul progetto di secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla ciber-criminalità (Convenzione di Budapest), sottolineando in particolare l'importanza di dotarsi di un regime di protezione dei dati che garantisca l'efficienza del perseguimento penale e promuova nel contempo la protezione delle persone interessate dal trattamento dei dati.

Il Comitato ha partecipato ai lavori preliminari di due documenti adottati dal Comitato dei Ministri nel 2021. Uno dei documenti concerne la dichiarazione del Comitato ministeriale sulla protezione del diritto dei bambini alla vita privata nell'ambiente digitale, elaborata dal comitato direttivo per i diritti del bambino del Consiglio d'Europa in collaborazione con il Comitato consultivo. La dichiarazione invita gli Stati membri a rafforzare la protezione della sfera privata e dei dati personali dei bambini, specie i loro dati sanitari e i dati rilevati nel settore dell'istruzione. Con particolare riferimento al contesto pandemico, si tratta di ridurre le ripercussioni potenzialmente negative dell'identificazione pubblica di un bambino contagiato dal COVID-19.

L'altro documento concerne la raccomandazione sulla protezione delle persone fisiche in relazione al trattamento di dati personali nel contesto della profilazione. Questa raccomandazione prevede che il rispetto dei diritti e delle libertà fondamentali nel settore pubblico e



privato sia garantito in tutte le operazioni di profilazione. Sostituisce la precedente dichiarazione del 2010 per tener conto del progresso tecnologico degli ultimi anni e armonizza il testo con la Convenzione 108 sulla protezione dei dati modernizzata, conosciuta come «Convenzione 108+».

Nella sua dichiarazione «Vaccinazione, certificati COVID-19 e protezione dei dati» il Comitato ha ricordato l'importanza di assicurare un equilibrio tra la protezione dei diritti e delle libertà fondamentali e le sfide di salute pubblica poste dalla pandemia.

Il Comitato ha altresì adottato linee guida relative alla protezione delle persone nel trattamento di dati personali nell'ambito di campagne politiche. Tali linee guida disciplinano l'applicazione della Convenzione sulla protezione dei dati modernizzata («108+») alle campagne politiche tenuto conto del crescente uso di strategie di campagna digitale messe in atto dai social media.

Il Comitato ha pure deciso di aggiornare il contratto standard del Consiglio d'Europa atto a garantire una protezione adeguata nel contesto dei flussi di dati transfrontalieri. I lavori in cui la Svizzera svolge il ruolo di relatrice sono ancora in una fase iniziale.

Migliorare la collaborazione con le autorità preposte alla protezione dei dati

[L'IFPDT ha partecipato come di consueto all'European Case Handling Workshop \(workshop europeo sul trattamento dei reclami\), organizzato questa volta dall'autorità di protezione dei dati di Gibilterra.](#)

A causa della pandemia l'evento si è svolto online il 16 e 17 novembre 2021. Vi hanno preso parte più di 120 rappresentanti di 30 autorità di protezione dei dati. Sono state discusse questioni relative alla notifica delle violazioni della protezione dei dati, al trattamento interno dei reclami e all'applicazione delle misure. Si è inoltre discusso delle ripercussioni della sentenza della Corte di giustizia europea, comunemente denominata «Schrems II». L'obiettivo dell'evento era quello di migliorare la collaborazione tra autorità per la protezione dei dati e soprattutto di renderla più efficiente.

Il workshop sul trattamento dei reclami ha un grande valore pratico, in particolare per le autorità di vigilanza minori. Offre una piattaforma nell'ambito della quale le autorità possono scambiare le loro esperienze e competenze. In vista dell'entrata in vigore della nuova legge sulla protezione dei dati (cfr. tema prioritario I) e dell'assistenza amministrativa ivi prevista, questo scambio e sviluppo del know how saranno importanti per l'IFPDT. Quest'ultimo si è pertanto offerto di organizzare il workshop in Svizzera nell'autunno 2023.

Incontro virtuale di oltre 90 membri e osservatori

La 43ª Assemblea mondiale per la protezione della vita privata (AMVP), precedentemente denominata Conferenza internazionale dei commissari alla protezione dei dati e della vita privata, si è tenuta dal 18 al 21 ottobre 2021, per la seconda volta online a causa della crisi sanitaria.

La conferenza virtuale è stata organizzata in Messico dall'Istituto nazionale per la trasparenza, l'accesso all'informazione e la protezione dei dati personali (INAI) e ha visto la partecipazione di oltre 90 membri e osservatori, che hanno esaminato le principali sfide in materia di protezione dei dati. La conferenza aveva come tema la protezione della vita privata e dei dati con un approccio incentrato sull'essere umano.

Un diritto fondamentale

La 43ª sessione a porte chiuse dell'Assemblea mondiale per la protezione della vita privata (AMVP) è stata aperta da Elizabeth Denham, commissaria all'informazione del Regno Unito, che ha elogiato il lavoro della comunità di protezione della vita privata durante la pandemia ed espresso l'auspicio che l'Assemblea continui ad avere un simile impatto.

«L'obiettivo di questa conferenza è di fare in modo che si passi dalla protezione dei dati personali alla protezione della vita privata delle persone quale diritto fondamentale», ha dichiarato l'ospite della conferenza in Messico, Blanca Lilia Ibarra Cadena, presidente commissaria dell'Istituto nazionale per la trasparenza, l'accesso all'informazione e la protezione dei dati personali.

Durante la sessione a porte chiuse, sono state discusse e approvate alcune risoluzioni dalle quali emerge una visione condivisa su una serie di importanti temi d'attualità:

- la condivisione di dati per il bene pubblico;
- i diritti digitali dei bambini;
- l'accesso del governo ai dati;
- il futuro dell'AMVP;
- la cooperazione internazionale in materia di applicazione della legge
- e le regulatory sandbox.

Nuovo piano strategico

I partecipanti alla Conferenza hanno adottato un nuovo piano strategico biennale per l'AMVP volto a creare un ambiente che permetta alle autorità di protezione dei dati e della vita privata di assolvere concretamente il loro mandato, vale a dire assicurare norme elevate di protezione dei dati su scala mondiale come pure promuovere e agevolare una cooperazione efficace in materia di regolamentazione.

L'AMVP ha pure annunciato i vincitori dei premi mondiali sulla protezione della vita privata e dei dati nel 2021. Questi riconoscimenti sottolineano quanto realizzato dai responsabili mondiali della protezione della vita privata ed evidenziano le indagini particolarmente significative, le buone pratiche e le iniziative volte a sensibilizzare il pubblico.

Protezione dei dati nell'aiuto internazionale allo sviluppo

Un anno dopo la sua costituzione, il Gruppo di lavoro sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione di crisi (GT AID) stila un primo bilancio delle sue attività.

Il Gruppo di lavoro sul ruolo della protezione dei dati personali nell'aiuto internazionale allo sviluppo, nell'aiuto umanitario internazionale e nella gestione di crisi (GT AID) è stato istituito in seguito a una risoluzione dell'Assemblea mondiale per la protezione della vita privata (AMVP) adottata nella sua 42ª conferenza annuale nel 2021. Presieduto dall'IFPDT, il GT AID conta oltre 20 membri e la sua composizione rispecchia la varietà geografica dell'AMVP.

Nel corso del suo primo anno di attività, il GT AID si è concentrato sull'elaborazione di un piano di lavoro in sintonia con le priorità strategiche dell'AMVP che riguardano in particolare:

- l'avanzamento della protezione della vita privata su scala mondiale;

- il rafforzamento delle relazioni con altri organismi e reti internazionali che promuovono le questioni legate alla protezione dei dati e della vita privata, anche mediante accordi con gli organismi che giocano un ruolo di osservatore;
- i diritti della persona, la protezione sociale e i diritti democratici.

Obiettivi generali

Conformemente alle priorità poste nella risoluzione, i membri del GT AID si sono posti i seguenti obiettivi generali:

- rispondere alla domanda di cooperazione degli attori interessati (p. es. agenzie di sviluppo, attori umanitari) per sviluppare linee direttrici e promuovere lo scambio di buone pratiche in materia di protezione dei dati personali e della vita privata, tenuto conto delle specificità dell'aiuto internazionale allo sviluppo, dell'azione umanitaria internazionale e della necessità di agevolare queste attività;
- sviluppare una strategia di patrocinio e mobilitazione presso gli attori interessati.

Allo scopo di raggiungere questi obiettivi, il GT AID ha deciso di mettere in atto attività che permettano di:

- migliorare la comprensione dell'aiuto internazionale allo sviluppo, dell'aiuto umanitario internazionale e della gestione di crisi;
- stabilire un contatto permanente con gli attori interessati a livello sia bilaterale sia multilaterale e ampliare di conseguenza la portata della voce

dell'AMVP rafforzando le relazioni con gli attori dell'aiuto internazionale allo sviluppo;

- collaborare con gli altri gruppi di lavoro dell'AMVP per produrre documenti e strumenti di patrocinio per garantire maggiore attenzione alla protezione dei dati personali e della vita privata nelle attività interessate;
- promuovere e agevolare, per i Paesi beneficiari di queste attività che non sono dotati di un quadro di protezione dei dati personali e della vita privata, la loro integrazione nella comunità internazionale della protezione dei dati personali e della vita privata.

Nell'ambito di queste attività, i membri del GT AID hanno elaborato una cartografia dell'aiuto internazionale allo sviluppo e dell'aiuto umanitario internazionale. Hanno parimenti identificato i Paesi beneficiari di queste attività che non sono dotati di un quadro di protezione dei dati personali e della vita privata. Inoltre, il GT AID ha redatto un questionario e una lettera d'accompagnamento che gli permetterà di comprendere meglio il lavoro degli attori interessati.

SISTEMI D'INFORMAZIONE SCHENGEN

Gruppi di coordinamento di vigilanza dei sistemi SIS II, VIS ed Eurodac

I Gruppi di coordinamento di vigilanza dei sistemi SIS e VIS hanno finalizzato una lettera congiunta sulla proposta legislativa della Commissione europea di adeguamento del meccanismo di valutazione di Schengen.

Come già lo scorso anno, a causa della situazione pandemica entrambe le sedute dei tre gruppi di coordinamento di vigilanza dei sistemi d'informazione UE SIS II, VIS (presidenza IFPDT) ed Eurodac si sono svolte in videoconferenza. La prima si è tenuta il 16 e 17 giugno 2021 mentre la seconda il 24 e 25 novembre 2021. Vi hanno partecipato il Garante europeo della protezione dei dati (GEPD) e le autorità nazionali incaricate della protezione dei dati degli Stati membri.

Il Gruppo di coordinamento di vigilanza del sistema VIS ha finalizzato un questionario sulla cancellazione anticipata dei dati nel caso in cui una persona acquisisce la nazionalità di uno Stato membro e quindi non necessita più di un visto Schengen. Le autorità di protezione dei dati degli Stati membri sono ora invitate a fare compilare il questionario nei loro Stati per valutare l'attuazione della cancellazione anticipata nei diversi Stati.

Durante la seduta del mese di novembre i gruppi di coordinamento di vigilanza dei sistemi SIS e VIS hanno finalizzato una lettera congiunta

sulla proposta legislativa della Commissione europea di adeguamento del meccanismo di valutazione di Schengen. Nello scritto sottolineano in particolare l'importanza di coinvolgere nelle valutazioni Schengen riguardanti la protezione dei dati soprattutto esperti delle autorità di protezione dei dati. Nel contempo è stato ribadito che si dovrebbe ricorrere agli esperti prima del previsto, ossia quattro mesi prima e non soltanto undici settimane. La lettera è stata inviata al Consiglio, alla Commissione e al Parlamento dell'Unione europea.

Assieme all'Agenzia dell'UE per i diritti fondamentali (European Union Agency for Fundamental Rights, FRA) l'Eurodac SCG ha adottato una guida sul diritto all'informazione nel contesto del rilevamento delle impronte digitali per Eurodac, guida destinata alle autorità. Il documento è stato distribuito alle competenti autorità svizzere e pubblicato su diverse pagine internet.

REGNO UNITO

Brexit – Adeguatezza della protezione dei dati

Dal punto di vista della Svizzera permane invariato lo statuto di adeguatezza del Regno Unito. Quest'ultimo figura infatti ancora nell'elenco compilato dall'IFPDT come Paese con un livello di protezione dei dati equivalente.



SISTEMI DI VIDEOCONFERENZA

Buone pratiche delle autorità incaricate della protezione dei dati

Dall'inizio della pandemia le autorità e le imprese private hanno utilizzato sempre più le piattaforme di videoconferenza. In collaborazione con cinque autorità di protezione dei dati di altri Paesi l'IFPDT ha offerto alle società di videoconferenza Microsoft, Google, Cisco e Zoom la possibilità di presentare le loro piattaforme di videoconferenza e di aprire un dialogo trasparente con le autorità.

Gli scambi intrattenuti con le società di videoconferenza si sono concentrati sui seguenti temi: sicurezza, «Privacy by design and default», «Know your audience» e trasparenza. Il dialogo si è rivelato utile per tutte le parti coinvolte. Ne è risultata una dichiarazione concernente le «buone pratiche», disponibile sul sito Internet dell'IFPDT. Qui di seguito abbiamo selezionato alcune delle misure contenute (cfr. riquadro).

È inoltre importante che i fornitori di servizi di videoconferenza costruiscano una fiducia nei confronti dei loro utenti trattando soltanto le informazioni su di loro che possono aspettarsi

dalle circostanze. I dati personali dovrebbero essere raccolti solo nella misura in cui sono necessari per l'utilizzo delle funzioni principali del servizio di videoconferenza. Gli utenti devono essere messi al corrente, in modo completamente trasparente, sul luogo in cui i dati sono salvati e sui canali attraverso cui sono trasportati. Agli utenti dev'essere altresì data la possibilità di scegliere attraverso quali luoghi i loro dati personali vengono inoltrati e dove vengono memorizzati.

Il documento pubblicato sul sito Internet non è esaustivo. Motivo per cui le imprese che offrono servizi corrispondenti devono anche osservare le disposizioni sulla protezione dei dati applicabili in Svizzera e le spiegazioni dell'IFPDT sulla trasmissione di dati all'estero.

Sicurezza

- È indispensabile testare regolarmente le misure di sicurezza al fine di garantire che rimangano affidabili nonostante la costante evoluzione delle minacce.
- Occorre formare regolarmente i collaboratori sul tema della protezione dei dati e della sicurezza.
- È opportuno organizzare regolarmente audit di terzi, inclusa la registrazione dell'accesso di sotto-responsabili del trattamento di dati personali e il principio del minimo privilegio del controllo dell'accesso.

Trasparenza

- Gli utenti devono essere informati sulle modalità e sul motivo per cui i loro dati sono raccolti e utilizzati.
- Gli utenti devono essere chiaramente informati sulle terze parti con cui vengono condivisi i loro dati, nonché sul motivo.

Principi «Privacy by design» e «Privacy by default»

- Prima di implementare nuove soluzioni e funzionalità di videoconferenza occorre svolgere valutazioni d'impatto sulla protezione dei dati e garantire un contatto regolare fra i servizi incaricati della protezione dei dati, della sicurezza e dello sviluppo.
- Dev'essere rispettato il principio della minimizzazione dei dati.
- Le società di videoconferenza devono impostare gli standard di protezione dei dati in relazione ai loro servizi al livello più elevato.

«Know your audience»

- Le società di videoconferenza devono dotarsi di dispositivi di protezione dei dati e di sicurezza performanti per proteggere adeguatamente i dati personali in contesti sensibili, quali la formazione e la sanità.
- Occorre elaborare istruzioni specifiche in materia di protezione dei dati e di sicurezza in funzione del gruppo di utenza, affinché i requisiti di sicurezza nell'uso di un servizio di videoconferenza siano garantiti per tutti gli utenti, consentendo loro di scegliere le impostazioni e le funzioni più appropriate per loro.

Crittografia «end-to-end»

- È opportuno perseguire una crittografia «end-to-end» in cui l'host della sessione crea una chiave di cifratura in modo che soltanto lui stesso e i partecipanti abbiano accesso ai dati in questione.
- È importante l'uso standardizzato della crittografia end-to-end nelle conversazioni sensibili one-to-one, per esempio nel settore della telemedicina.

Comunicazione di dati all'estero

CLAUSOLE CONTRATTUALI TIPO (SCC)

Comunicazione di dati personali in un Paese senza un livello adeguato di protezione dei dati

Nel suo parere del 27 agosto 2021 l'IFPDT ha riconosciuto le clausole contrattuali tipo (Standard Contractual Clauses, SCC) dell'UE quale base per la comunicazione di dati personali in Paesi senza un livello adeguato di protezione dei dati. Per poterle utilizzare in base al diritto svizzero sulla protezione dei dati, l'IFPDT ha previsto opportune modifiche e aggiunte.

La legge svizzera sulla protezione dei dati prevede che i dati personali non possano essere comunicati in Paesi che non prevedono un livello adeguato di protezione dei medesimi. Sono possibili eccezioni se nel Paese destinatario può essere assicurata una protezione adeguata per esempio mediante garanzie contrattuali. Occorre però esaminare nei casi concreti di applicazione se gli accordi contrattuali consentono effettivamente di assicurare una protezione adeguata dei dati personali che devono essere comunicati. A tale scopo l'IFPDT mette a disposizione sul suo sito Internet una guida per l'esame dell'ammissibilità della comunicazione di dati all'estero.

Se per una comunicazione di dati è in linea di principio possibile ricorrere a una garanzia contrattuale, le clausole contrattuali tipo (Standard Contractual Clauses, SCC) adottate dalla Commissione europea nella decisione di esecuzione (EU) 2021/914 del 4 giugno 2021 rappresentano un mezzo adeguato.

Nel suo parere del 27 agosto 2021 l'IFPDT ha riconosciuto le nuove SCC e i relativi moduli, che si rifanno al Regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea, a condizione che siano se necessario adattati e/o completati nei casi concreti di applicazione. A tal proposito l'IFPDT spiega che dopo aver scelto lo scenario specifico (esportatore e importatore di dati possono essere sia responsabili sia incaricati del trattamento), si deve stabilire a quale diritto sottostà la comunicazione di dati: soltanto al diritto svizzero sulla protezione dei dati oppure sia al diritto svizzero sia a quello europeo. Da questa distinzione scaturiscono diversi adattamenti del contratto, in particolare per quanto riguarda l'autorità di vigilanza competente, il diritto applicabile per le pretese contrattuali e il foro. Trovate maggiori dettagli nel parere dell'IFPDT pubblicato sul suo sito Internet.

In base al diritto vigente l'utilizzo delle SCC riconosciute deve essere notificato all'IFPDT prima della comunicazione. Con la nuova legge sulla protezione dei dati quest'obbligo di notifica decadrà.

Schema per l'esame dell'ammissibilità secondo art.6 cpv.2 lett. a LPD

Dopo la sua presa di posizione dell'8 settembre 2020 in merito al regime dello scudo per la privacy, l'IFPDT ha pubblicato una guida per l'esame dell'ammissibilità della comunicazione di dati all'estero secondo l'articolo 6 capoverso 2 lettera a LPD. Se le garanzie contrattuali ed eventuali ulteriori misure di protezione non sono sufficienti, la comunicazione di dati all'estero è illegale.

La guida pubblicata dall'IFPDT sul suo sito Internet mira a facilitare ai responsabili l'esame dell'ammissibilità della comunicazione di dati all'estero. Mediante uno schema e il questionario allegato viene illustrato il caso in cui i dati sono comunicati in un Paese privo di una legislazione che assicuri una protezione adeguata e questa lacuna deve essere compensata o eliminata con altre garanzie sufficienti (art. 6 cpv. 2 lett. a LPD).

Se nell'elenco degli Stati dell'IFPDT un Paese è considerato non adeguato o non adotta la protezione per la comunicazione di dati in questione, dopo aver analizzato la prevista comunicazione di dati l'esportatore deve prevedere ulteriori misure come ad esempio accordi contrattuali con l'importatore. Di norma si tratta di clausole contrattuali tipo (Standard Contractual Clauses, SCC; cfr. testo sulle SCC a sinistra).

Quando si applicano le SCC occorre esaminare se queste siano già di per sé non sufficienti, ad esempio perché prevalgono norme non adeguate del diritto applicabile alla parte contraente. In questi casi si deve chiarire se le quattro garanzie sancite dal diritto fondamentale (principio di legalità,

principio di proporzionalità, possibilità di adire le vie legali e garanzia della via giudiziaria) sono assicurate nel diritto estero applicabile. Indicativamente l'IFPDT ha allegato alla guida un catalogo di domande adattato al diritto statunitense, che si basa sui questionari corrispondenti dell'organizzazione non governativa di Maximilian Schrems «My Privacy Is None Of Your Business» (noyb).

Se tutte le garanzie richieste sono assicurate dal diritto cui soggiace la parte contraente, le SCC sono sufficienti a meno che non siano necessarie ulteriori misure contrattuali di protezione. Potrebbe ad esempio trattarsi di norme che rafforzano i diritti degli interessati (ad esempio diritto d'accesso) o determinate misure tecniche come condizione per la comunicazione di dati.

Se invece queste garanzie non sono cumulativamente soddisfatte nell'ordinamento giuridico applicabile al partner contrattuale, l'esportatore deve considerare ulteriori misure di protezione contrattuali, organizzative e/o soprattutto tecniche. Se tali misure non consentono di compensare la mancanza di protezione, la comunicazione di dati all'estero è illegale e va quindi sospesa o cessata immediatamente.

Rischi e requisiti per l'utilizzo di cloud pubblici da parte delle autorità

Anche nell'anno in rassegna l'IFPDT si è occupato intensamente della tematica del cloud computing. Nell'ambito di consultazioni degli uffici e della consulenza fornita a un gruppo di lavoro dell'Amministrazione federale ha evidenziato i rischi e i requisiti di un'esternalizzazione del trattamento di dati personali a fornitori di cloud pubblici da parte delle autorità.

In merito all'interpellanza Andrey del 16 settembre 2021 («Aggiudicazione di servizi di cloud pubblico a ditte americane e cinesi») l'IFPDT ha richiamato l'attenzione del settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale sul fatto che, anche considerando l'acquisto «fiduciario» di servizi cloud da filiali europee, non sempre si può escludere l'applicabilità di disposizioni legali estere problematiche e quindi il rischio di accessi sproporzionati da parte delle autorità competenti. Ha inoltre osservato che, oltre a garantire la sicurezza dei dati, occorre assicurarsi che il fornitore di cloud sia tenuto a osservare il segreto d'ufficio. L'IFPDT ha infine sottolineato che, indipendentemente dalla destinazione, l'esternalizzazione di dati personali a terzi aumenta sempre i rischi per l'integrità, la disponibilità e la riservatezza dei dati, motivo per cui è indispensabile effettuare una valutazione d'impatto dei rischi.

L'IFPDT ha esposto il proprio parere al TDT anche in relazione all'interpellanza Marti del 30 settembre 2021 («Servizi cloud di Microsoft») rilevando che, in considerazione dei lavori in corso nell'Amministrazione, le decisioni determinanti sull'uso di servizi cloud di Microsoft o di altri

fornitori possono essere prese soltanto dopo un'analisi delle basi legali, l'elaborazione di un piano di sicurezza dell'informazione e di protezione dei dati, nonché un'analisi dei rischi che includa anche i rischi per la protezione dei dati. Abbiamo sottolineato la necessità di considerare offerte alternative tenuto conto che nel cloud, oltre ai dati telemetrici e ai dati dell'utente, vengono memorizzati potenzialmente anche contenuti testuali. A questo proposito abbiamo ricordato i requisiti della legislazione sulla protezione dei dati, che possono prevedere l'obbligo di adottare misure tecniche atte a impedire fattivamente accessi sproporzionati da parte delle autorità del Paese di destinazione.

L'IFPDT ha inoltre partecipato a titolo consultivo alle sedute di un gruppo di lavoro ad hoc, diretto dalla Sezione del diritto della CaF, che si occupa del rapporto sul quadro giuridico del cloud. Il rapporto rientra nella strategia cloud dell'Amministrazione federale ed è inteso a chiarire la base legale relativa all'uso di cloud pubblici da parte della stessa. Considerata la rapidità con cui i progetti dell'Amministrazione federale basati su soluzioni di cloud computing stanno prendendo forma, tale accertamento del quadro giuridico è urgentemente necessario.

Attualmente l'IFPDT, al pari delle altre autorità di protezione dei dati in Europa, sta sviluppando una prassi relativa all'esternalizzazione del trattamento di dati personali da parte delle autorità pubbliche, in particolare a fornitori di servizi di cloud pubblici statunitensi. Sebbene né il diritto dell'UE né le sentenze della CGUE siano applicabili in Svizzera, l'IFPDT tiene comunque conto degli sviluppi del diritto europeo nella concretizzazione della sua prassi, poiché nell'applicazione della legislazione federale sulla protezione dei dati aspira a raggiungere un livello di protezione dei dati paragonabile a quello dell'UE, in considerazione delle decisioni di adeguatezza reciproche dell'UE e della Svizzera. In questo contesto è significativo il fatto che a fine marzo 2022 la presidente della Commissione europea e il presidente degli Stati Uniti abbiano annunciato la loro comune intenzione di sostituire entro breve il regime dello scudo della privacy (cfr. 28° Rapporto d'attività, tema prioritario II) con un disciplinamento migliore.

SCHREMS II

Comitato europeo per la protezione dei dati (EDPB), Borders, Travel & Law Enforcement Expert Subgroup (BTLE ESG)

L'IFPDT ha colto l'occasione per intervenire in seno al Comitato europeo per la protezione dei dati (EDPB) in particolare sulle questioni relative a Schengen e per scambiare il proprio punto di vista con le altre autorità europee. Durante l'anno in rassegna l'attenzione si è concentrata sulle ripercussioni di Schrems II e sulle reazioni delle autorità preposte alla protezione dei dati a questa giurisprudenza.

L'IFPDT è stato attivo nel Borders, Travel & Law Enforcement Expert Subgroup (BTLE ESG), soprattutto nella prima metà dell'anno in rassegna. Il gruppo di lavoro si è occupato in modo approfondito della problematica correlata a Schrems II e ha elaborato raccomandazioni all'indirizzo dell'EDPB. Nel giugno 2021, dopo una consultazione pubblica, la riunione plenaria dell'EDPB ha adottato la versione finale delle raccomandazioni sulle misure supplementari. Esse mirano a sostenere i responsabili e i titolari del trattamento che esportano dati nella definizione e nella messa in pratica di misure supplementari adeguate. Tali misure possono rivelarsi necessarie per garantire ai dati personali trasmessi a Paesi terzi un livello di protezione sostanzialmente equivalente.

Il 18 giugno 2021 l'IFPDT ha pubblicato una guida basata sul diritto svizzero per l'esame dell'ammissibilità della comunicazione di dati all'estero (cfr. sopra, «Guida per l'esame dell'ammissibilità della comunicazione di dati all'estero secondo art. 6 cpv. 2 lett. a LPD»).

Principio di trasparenza

2.1 In generale

La legge sulla trasparenza ha lo scopo di promuovere la trasparenza sulle attribuzioni, l'organizzazione e l'attività dell'amministrazione. A tal fine contribuisce all'informazione del pubblico garantendogli accesso ai documenti ufficiali (cfr. art. 1 LTras). Il principio di trasparenza intende promuovere la fiducia nello Stato e nelle autorità rendendo comprensibile l'operato dell'Amministrazione e aumentando così l'accettazione dell'operato dello Stato.

Dalle cifre fornite dall'Amministrazione federale relative alle domande di accesso ai documenti ufficiali pervenute nel 2021 risulta che il bisogno espresso dai media e dalla società di avere un'informazione specifica e trasparente continua a essere grande. Anche nell'anno in rassegna sono state presentate alle autorità federali più domande di accesso che nell'anno precedente. Anche nel secondo anno della pandemia le richieste, spesso voluminose e complesse, hanno riguardato in quasi un caso su quattro documenti ufficiali relativi al coronavirus.

In molti casi il trattamento delle domande di accesso ha comportato un notevole impiego di risorse, non da ultimo perché spesso si è rivelato necessario un coordinamento fra gli uffici o i dipartimenti. Nel complesso è emerso che l'attuazione del principio di trasparenza in tempi di pandemia rimane arduo e impegnativo. Dalle cifre che seguono (cfr. n. 2.2) si evince che le tendenze constatate negli ultimi anni – un continuo aumento delle domande di accesso e una percentuale costantemente elevata di casi in cui il diritto d'accesso è completamente accordato – possono essere confermate anche per l'anno in rassegna.

Se le parti richiedenti o terzi interessati dalla concessione dell'accesso non concordano con l'intenzione delle autorità di accordarlo, la legge sulla trasparenza offre loro la possibilità di presentare all'Incaricato una domanda di mediazione. Anche qui si riconosce una chiara tendenza: nell'anno in rassegna l'Incaricato ha registrato 149 domande di mediazione pervenute, il 60 per cento in più rispetto all'anno precedente.

Obiettivo della procedura di mediazione è trovare rapidamente un compromesso tra gli interessati. Le misure introdotte a questo scopo con il progetto pilota nel 2017 e in particolare il primato dei negoziati di mediazione orali si sono dimostrati validi anche nel 2021. Dall'analisi delle domande di mediazione elaborate nel

2021 si evince che, quando è stato possibile effettuare una seduta di mediazione, si è giunti a una soluzione consensuale nel 67 per cento dei casi. Nelle 40 procedure di mediazione in cui si è dovuto rinunciare a una seduta a causa della pandemia è stato invece possibile giungere a un compromesso soltanto nel cinque per cento dei casi. Dopo che il 13 gennaio 2021 il Consiglio federale, in considerazione della situazione epidemiologica tesa, aveva introdotto tra l'altro l'obbligo del telelavoro e limitato a cinque persone gli assembramenti nello spazio pubblico, tutto ciò si è ripercosso direttamente anche sul modo di svolgere la procedura di mediazione. Tra gennaio e giugno 2021 l'Incaricato si è così visto costretto a rinunciare a condurre le sedute di mediazione in presenza degli interessati. In numerosi casi la procedura di mediazione è stata svolta per iscritto. Nell'anno in rassegna ciò non soltanto è stato all'origine di una percentuale ridotta di soluzioni consensuali, ma ha pure allungato la durata di elaborazione delle procedure e causato ritardi nella loro esecuzione (cfr. n. 2.3).

Dalle cifre esaminate emerge chiaramente che condurre sedute di mediazione in loco alla presenza degli interessati contribuisce ad accelerare lo

svolgimento delle procedure. Il numero di domande di mediazione, da anni in costante aumento, e l'accresciuta complessità delle richieste fanno tuttavia sì che l'Incaricato superi il termine di disbrigo di 30 giorni previsto dalla legge in una percentuale delle procedure sempre più elevata. L'Incaricato presuppone che, senza risorse supplementari, questa evoluzione negativa si acutizzerà ulteriormente e lo svolgimento rapido delle procedure, così come richiesto dal legislatore, continuerà ad accusare ritardi (cfr. in proposito le informazioni specifiche nel n. 2.3).

Negoziati per l'acquisto di vaccini anti-COVID-19

Ha suscitato un grande interesse pubblico la raccomandazione dell'Incaricato del 18 gennaio 2022 risalente a una domanda di mediazione presentata l'anno precedente (in ted. sul sito dell'Incaricato). L'Incaricato raccomandava all'UFSP di concedere l'accesso ai negoziati per l'acquisto di vaccini anti-COVID-19 dopo aver sentito le imprese farmaceutiche interessate e nel rispetto del principio di proporzionalità. Nella sua raccomandazione, dettagliatamente motivata, l'Incaricato evidenziava che doveva tener conto delle mutate condizioni nel caso di una valutazione ripetuta di eccezioni che motivassero il differimento dell'accesso. Poiché l'UFSP stesso aveva detto che la scarsità iniziale di vaccini non sussisteva nel frattempo più, l'Incaricato non

ravvisava alcun motivo per differire ulteriormente il trattamento delle domande di accesso pervenute anche in considerazione del fatto che la necessaria audizione delle imprese farmaceutiche avrebbe richiesto molto tempo. Questa raccomandazione dell'Incaricato è in linea con la decisione del Parlamento di rinunciare a sancire in una legge speciale, come invece auspicato dal Consiglio nazionale, un obbligo di pubblicazione dei negoziati per l'acquisto dei vaccini in questione. Come emerge anche dalle trattazioni in seno al Consiglio degli Stati, in assenza di un disciplinamento speciale si applica la legge sulla trasparenza. In applicazione proprio di questa legge l'Incaricato ha raccomandato anche di concedere l'accesso differito dall'UFSP.

2.2 Domande di accesso. Nuovo aumento nel 2021

Secondo le cifre comunicate dalle autorità federali, nell'anno in rassegna sono pervenute 1385 domande di accesso (nel 2020 erano 1193), pari a un aumento del 16 per cento rispetto al 2020. In 694 casi (il 50 %) le autorità hanno concesso accesso completo ai documenti (nel 2020: 610, pari al 51 %), mentre in 324 casi (23 %) un accesso parziale o differito (nel 2020: 293, pari al 25 %). In 126 casi (9 %) la consultazione è stata del tutto negata (nel 2020: 108, pari al 9 %). Secondo i dati forniti dalle autorità, 48 domande di accesso sono state ritirate (nel 2020: 35, pari al 3 %), 78 erano ancora pendenti alla fine del 2021 e in 115 casi non esisteva nessun documento ufficiale.

Ha contribuito ad aumentare il numero delle domande di accesso presentate anche il fatto che, grazie ai media, la popolazione conosce sempre meglio il principio di trasparenza e sfrutta attivamente in misura crescente anche le possibilità che offre. Si presuppone che la tendenza sia destinata a continuare anche nei prossimi anni.

Un ulteriore motivo per l'aumento delle domande di accesso è da ricondurre al bisogno di trasparenza e di informazione andato di pari passo con le misure introdotte nel corso della pandemia di coronavirus. Le autorità hanno potuto rilevare statisticamente le domande di accesso ai «documenti COVID» e trasmetterle all'Incaricato assieme ai dati da fornire su base annuale (cfr. Statistica delle domande

di accesso 2021 con riferimento a Corona). Secondo i dati delle autorità federali, 336 delle complessive 1385 domande di accesso (24 %) avevano un legame con il coronavirus. In questo caso l'accesso completo è stato concesso in 121 casi (36 %), quindi con minore frequenza rispetto alla statistica globale. Sempre per quanto riguarda i documenti COVID le autorità hanno deciso un accesso limitato o differito in 131 casi (39 %), quindi più spesso, mentre con 13 casi (4 %) in cui l'accesso è stato negato la quota risulta più che dimezzata rispetto alla statistica globale. 18 domande di accesso sono state ritirate, 29 erano ancora pendenti alla fine del 2021 e in 24 casi non esisteva alcun documento ufficiale. Si prevede che l'elaborazione sociale delle misure amministrative adottate contro la pandemia si protrarrà oltre il termine auspicato di superamento della crisi sanitaria, cosicché nel 2022 dovrebbero pervenire ulteriori domande di accesso e di mediazione collegate alla pandemia.

In sintesi l'Incaricato constata che dal 2015 è concesso un accesso completo ai documenti in almeno il 50 per cento dei casi, mentre nel corso degli anni l'accesso è stato negato nel quasi dieci per cento dei casi.

Dipartimenti e uffici federali

Nel 2021, e quindi nel secondo anno della pandemia di coronavirus, singole unità amministrative si sono trovate nuovamente al centro dell'interesse dei media e della società. Dati i compiti che svolgono, soprattutto il DFI e il DDPS si sono visti confrontati con un gran numero di domande di accesso. Nel caso del DFI, il 63 per cento delle domande chiedeva a livello interdipartimentale l'accesso a documenti ufficiali inerenti al coronavirus. Secondo le autorità si trattava in parte di domande molto voluminose e complesse. In numerosi casi è stato necessario organizzare un dispendioso coordinamento interno tra gli uffici o i dipartimenti. Per queste autorità l'onere amministrativo è stato maggiore rispetto al periodo precedente al coronavirus, circostanza che – come menzionato – potrebbe proseguire anche nel 2022.

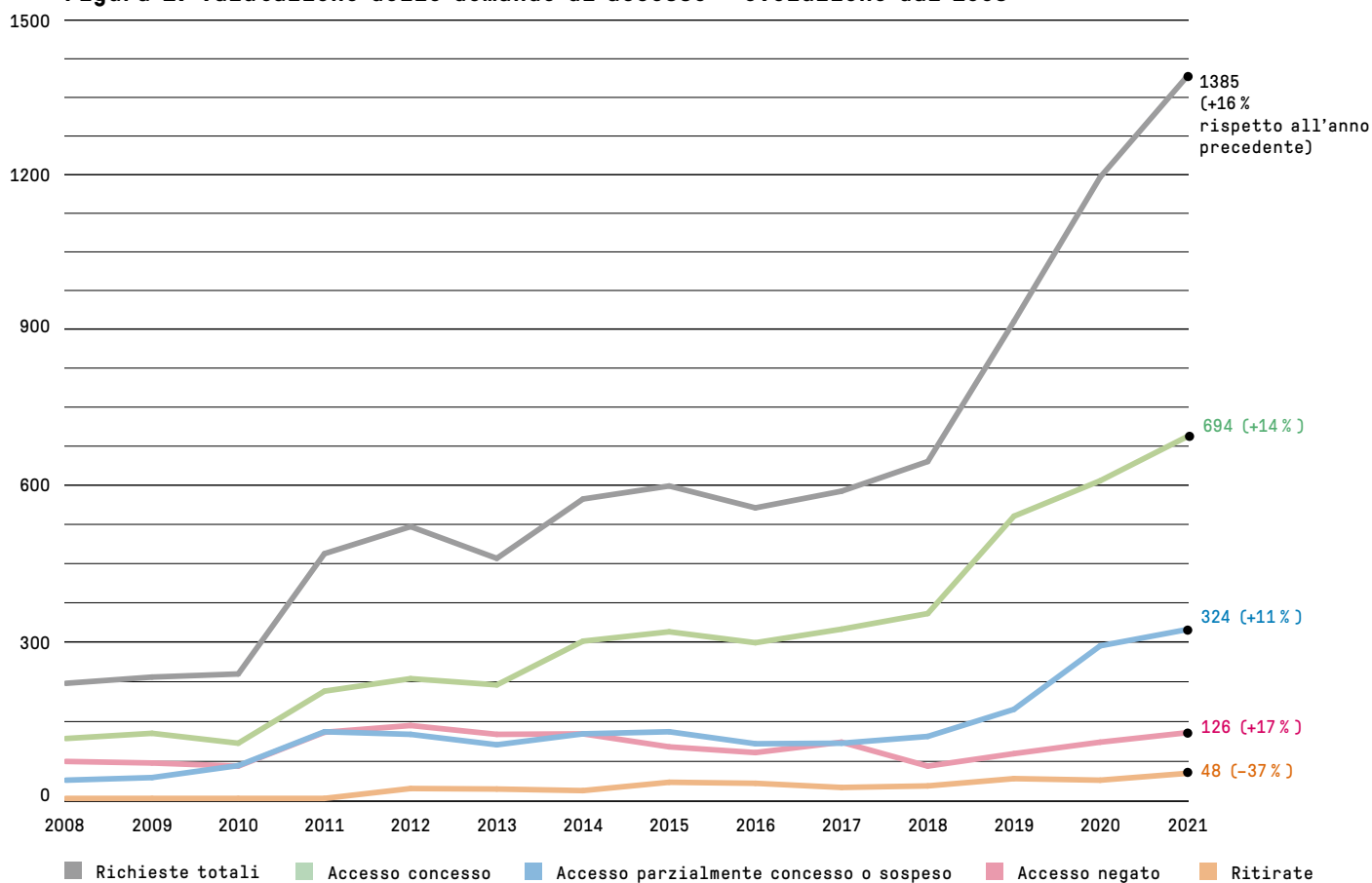
A livello di ufficio, dalle cifre comunicate si evince che, con 251 casi nell'anno in rassegna, l'UFSP ha segnalato il maggior numero di domande di accesso pervenutegli, di cui ben

217 riguardavano documenti relativi al coronavirus. Seguono l'UFSPPO con 172, swissmedic con 72 e l'UFAM con 64. A livello di dipartimento sono in testa il DFI (422), il DDPS (281) e il DFAE (156). Tredici autorità hanno segnalato di non aver ricevuto nessuna domanda di accesso nell'anno in rassegna. All'incaricato stesso sono giunte 16 domande di accesso e in sette casi ha concesso l'accesso completo. In due casi l'accesso è stato concesso in modo limitato o differito e in due casi completamente negato. Cinque domande erano ancora pendenti alla fine del 2021.

L'importo degli emolumenti riscossi nel 2021 per l'accesso ai documenti ufficiali ammonta a un totale di 14 924,90 franchi, poco al di sotto quindi dell'importo dell'anno precedente (15 189,30 fr.). Mentre il DFAE, il DATEC, i Servizi del Parlamento e il Ministero pubblico non hanno riscosso alcun emolumento, gli altri cinque dipartimenti e la Cancelleria federale hanno fatturato ai richiedenti una

parte del tempo impiegato (DFI: 7665,20 fr.; DEFR: 4052,70 fr.; CaF: 1150 fr.; DDPS: 950 fr.; DFF: 750 fr.; DFGP: 357 fr.). Si noti al riguardo che soltanto per 19 delle 1385 domande di accesso presentate è stato riscosso un emolumento. Rispetto all'anno precedente, in cui in 25 casi era stato richiesto un emolumento, ciò rappresenta un calo, sia per quanto riguarda i casi in cui è stato riscosso un emolumento sia per quanto riguarda l'importo totale degli emolumenti. Questo aspetto è degno di nota perché il numero delle

Figura 1: valutazione delle domande di accesso – evoluzione dal 2008





domande di accesso è considerevolmente aumentato. Come già negli anni precedenti, la riscossione di emolumenti rimane un'eccezione: oltre il 98 per cento delle domande di accesso è esente da emolumenti. La prassi amministrativa applicata anche nell'anno in rassegna, secondo cui i documenti ufficiali possono essere consultati per principio gratuitamente, deve essere sancita nella legge. Il 1° dicembre 2021 anche il Consiglio degli Stati, dopo il Consiglio nazionale, è entrato in materia su un'iniziativa parlamentare pertinente secondo cui in futuro le domande saranno a pagamento soltanto se la loro elaborazione comporterà oneri particolarmente elevati per le autorità. Sarà ora il Parlamento a decidere sulla definizione concreta e sull'attuazione del principio dell'esenzione dagli emolumenti e su eventuali eccezioni nell'accesso ai documenti ufficiali.

Per quanto riguarda il tempo impiegato per il trattamento delle domande di accesso, l'Incaricato rammenta nuovamente che le autorità non sono tenute a registrarlo e che non esistono prescrizioni applicabili all'intera Amministrazione federale per una registrazione uniforme. I dati fornitigli su base volontaria rispecchiano quindi soltanto in parte le ore di lavoro effettivamente prestate. Secondo tali dati, il tempo impiegato nell'anno in rassegna, ossia 5562,35 ore, è aumentato rispetto al 2020 (5010 ore).

Che l'onere annunciato dalle autorità per elaborare le domande di accesso corrisponda soltanto in parte al tempo effettivamente impiegato lo si riconosce a titolo di esempio dai dati forniti dall'UFSP. Oltre al tempo impiegato comunicato periodicamente dalle unità specializzate responsabili dell'UFSP (208,5 ore) e al supporto giuridico offerto dalla sua incaricata del principio di trasparenza, corrispondente a un tasso d'occupazione del 40 per cento, l'UFSP ha annunciato l'istituzione di una propria struttura d'esecuzione nonché di processi specifici intesi a elaborare le numerose domande di accesso in relazione al COVID-19. Secondo i dati forniti dall'UFSP l'onere nell'anno

in rassegna è stato molto elevato ed è ammontato almeno a 3,9 equivalenti a tempo pieno (Full Time Equivalent). Qualcosa di simile dovrebbe valere per altre unità dell'Amministrazione federale.

Un aumento si constata anche nel caso del tempo necessario per preparare le procedure di mediazione segnalato: 864,6 ore (rispetto alle 569 ore nel 2020, 473 nel 2019, 672 nel 2018 e 914 nel 2017).

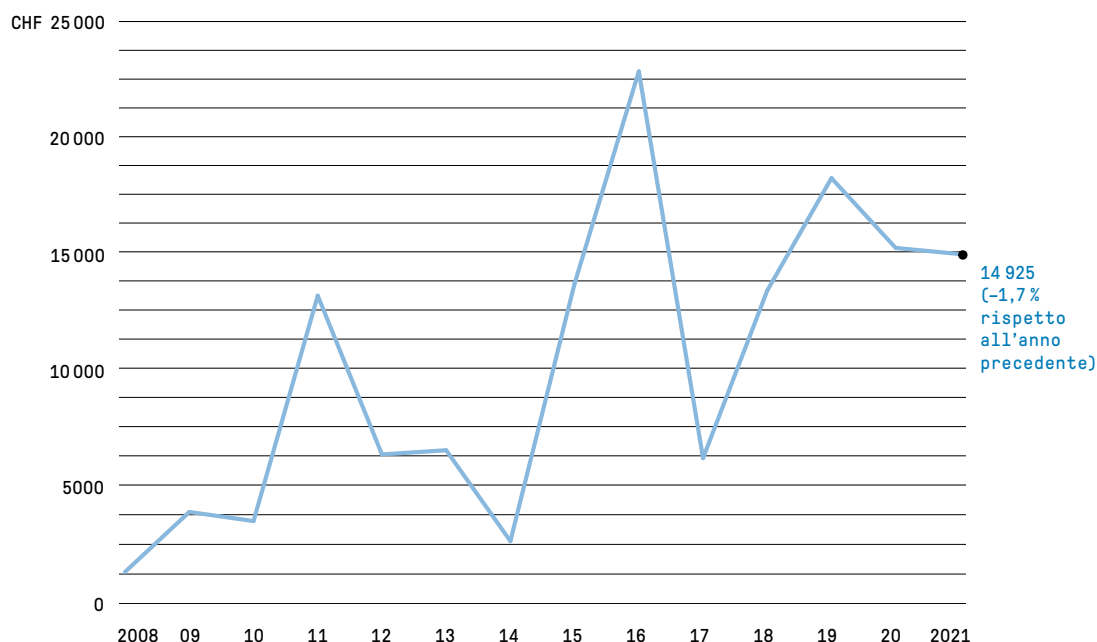
Servizi del Parlamento

I Servizi del Parlamento hanno comunicato di aver ricevuto una domanda di accesso che è stata approvata e l'accesso ai documenti richiesti è stato concesso completamente.

Ministero pubblico della Confederazione

Il Ministero pubblico della Confederazione ha comunicato la ricezione di otto domande nel 2021. In quattro casi l'accesso è stato completamente negato, in uno la domanda di accesso è stata ritirata. Per le altre tre domande non erano disponibili documenti ufficiali.

Figura 2: emolumenti riscossi dall'entrata in vigore della LTras



2.3 Procedure di mediazione: aumento significativo delle domande di mediazione

Nel 2021 all'Incaricato sono state presentate 149 domande di mediazione, un aumento del 60 per cento rispetto alle 93 ricevute nel 2020. La maggior parte di esse è stata presentata da giornalisti (53) e privati (49). Da queste cifre si può constatare che nei 565 casi in cui il Ministero pubblico della Confederazione ha rifiutato completamente o in parte l'accesso oppure l'ha differito o ha dichiarato che non erano disponibili documenti ufficiali, per 149 volte, ossia nel 26 per cento dei casi, è stata presentata una domanda di mediazione. Di queste domande, 31 (21%) riguardavano documenti ufficiali connessi al coronavirus.

Nel 2021 si sono potute evadere 139 domande di mediazione, di cui 126 pervenute nello stesso anno e 13 in quello precedente. In 50 casi è stato possibile giungere a una soluzione

consensuale. L'Incaricato ha inoltre emesso 49 raccomandazioni che hanno portato alla conclusione di 63 casi per i quali non era stato possibile giungere a una soluzione consensuale.

Tra i casi risolti vanno annoverate anche sette domande che non sono state presentate entro il termine previsto, 17 casi in cui non sono stati soddisfatti i requisiti per l'applicazione della legge sulla trasparenza nonché due domande di mediazione che sono state ritirate.

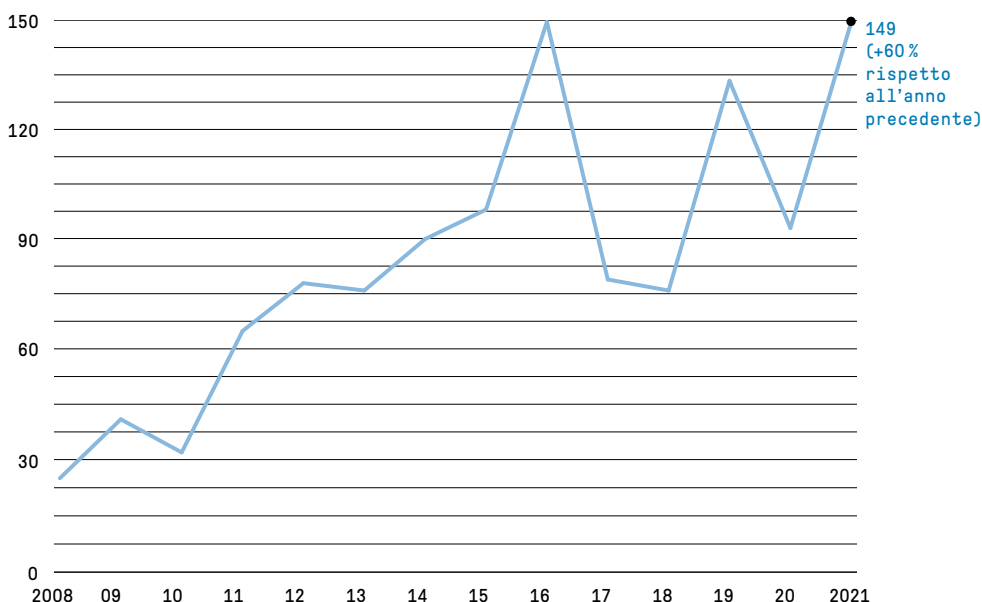
A fine anno otto procedure di mediazione risultavano sospese, previo accordo tra le parti o su loro richiesta.

Percentuale di soluzioni consensuali

Le soluzioni consensuali presentano numerosi vantaggi: consentono di chiarire la situazione e di accelerare la procedura di accesso nonché di creare la base per un'eventuale futura collaborazione tra i partecipanti alla seduta di mediazione.

L'efficacia delle misure introdotte nel 2017 e dello svolgimento delle sedute di mediazione orali è dimostrata soprattutto dalla proporzione esistente tra le soluzioni consensuali e le raccomandazioni. Nell'anno in rassegna è stato possibile pervenire a 50 soluzioni consensuali e l'Incaricato ha emesso 49 raccomandazioni per risolvere 63 casi, il che corrisponde al 44 per cento di

Figura 3: richieste di mediazione dall'entrata in vigore della LTras



soluzioni consensuali rispetto alle raccomandazioni. A tal proposito occorre tuttavia chiarire che normalmente una soluzione consensuale può essere conseguita soltanto se è possibile tenere una seduta di mediazione. Nell'anno in rassegna, nelle 45 sedute di mediazione svolte si è potuti giungere a un compromesso in 30 casi (67%). Come già menzionato nel numero 2.1, le misure poste in vigore per contenere il coronavirus hanno fatto sì che nel periodo compreso tra gennaio e giugno 2021, e quindi in 40 casi, si è stati costretti a rinunciare a condurre sedute di mediazione alla presenza fisica degli interessati. Non sono così mancate le ripercussioni sulla percentuale delle soluzioni consensuali: soltanto in due delle procedure scritte (5%) si è potuti giungere a un compromesso.

Da quanto esposto sopra si constata quindi che le sedute di mediazione orali continuano a risultare efficaci per giungere a soluzioni consensuali. L'Incaricato ritiene che questo modo di procedere sia ancora da preferire e da promuovere rispetto alla procedura scritta. Effettuare sedute di mediazione orali è vantaggioso per tutte le parti interessate. In alcuni casi, in considerazione delle misure per la lotta alla pandemia, le

parti alla procedura hanno chiesto di sospenderla finché non fosse di nuovo possibile svolgere sedute in presenza.

Nota: tutte le raccomandazioni dell'anno in rassegna sono disponibili sul sito dell'Incaricato (www.lincariato.ch).

Tabella 1: soluzioni consensuali

2021 (Corona)	44%
2020 (Corona)	34%
2019	61%
2018	55%

Durata delle procedure di mediazione

La tabella 2 sottostante è suddivisa in tre colonne in base alla durata della procedura. Per maggiore precisione si noti che la durata di elaborazione non

tiene conto del periodo in cui una procedura di mediazione è sospesa su proposta e previo accordo dei partecipanti. Una sospensione della procedura di mediazione si verifica in particolare quando, dopo la seduta, un'autorità desidera riconsiderare la propria posizione o se deve sentire terzi interessati. Se la seduta viene differita su richiesta di una parte interessata (p. es. a causa di assenza per vacanze, malattia ecc.), anche il periodo che intercorre tra il termine previsto inizialmente e il nuovo termine fissato o il conseguente prolungamento della procedura non è conteggiato nella durata di elaborazione.

Dalla tabella 2 si evince che il 42 per cento delle procedure di mediazione concluse nel 2021 è stato elaborato entro il termine ordinario di 30 giorni. Nel 51 per cento dei casi la procedura di mediazione è durata tra 31 e 99 giorni e nel sette per cento dei casi persino più di 100 giorni.

Di norma, il termine legale di 30 giorni per svolgere procedure di mediazione può essere rispettato se le sedute di mediazione vengono concluse con successo mediante un compromesso, ossia senza una richiesta di rinvio da parte dei partecipanti, entro il termine successivo al ricevimento della domanda. Nel caso in cui la procedura si è conclusa con un compromesso, nell'anno in rassegna il termine di 30 giorni è stato rispettato nel 60 per cento dei casi.

L'elevato numero delle domande di mediazione presentate all'Incaricato nel 2021 ha fatto sì che già all'arrivo della domanda fosse chiaro che non era possibile rispettare il termine di 30 giorni. A causa della scarsità di personale disponibile per elaborare le domande di mediazione, non è stato possibile fissare la seduta prima che scadesse il termine.

Si noti inoltre che delle 59 domande di mediazione elaborate entro il termine di 30 giorni, soltanto in 31 casi (53%) la procedura si è conclusa con un compromesso o una raccomandazione e di conseguenza ha avuto luogo un esame materiale dell'oggetto della mediazione. Nei rimanenti 28 casi (47%) non vi è stato alcun giudizio materiale nel merito; si è trattato in particolare di casi situati al di fuori del campo di applicazione della legge sulla trasparenza o in cui mancavano i requisiti formali per avviare una procedura di mediazione.

Come già menzionato, nel periodo compreso tra gennaio e giugno 2021 non si sono potute svolgere sedute di mediazione in loco a causa della pandemia. Di conseguenza, le procedure di mediazione che si sarebbero dovute svolgere in questo lasso di tempo hanno potuto concludersi soltanto in pochi casi (5%) con una soluzione consensuale. Se non si giunge a un compromesso, l'Incaricato deve emettere una raccomandazione scritta. Il fatto che la procedura di mediazione venga svolta per iscritto e che occorra elaborare una raccomandazione causa regolarmente all'Incaricato un carico di lavoro nettamente maggiore. Ne consegue che l'elaborazione delle singole procedure dura tendenzialmente più a lungo, comportando ripercussioni su

tutte le procedure susseguenti e sulla loro rispettiva durata. In questo senso anche i disciplinamenti introdotti a causa della pandemia di coronavirus sono stati all'origine di una maggiore durata delle procedure e di ritardi nell'elaborazione delle medesime. Se si è già in presenza di ritardi, ogni nuova domanda presentata contribuisce ad aumentarli. Nell'anno in rassegna l'Incaricato è riuscito a far pervenire ai partecipanti la raccomandazione scritta entro 30 giorni dalla ricezione della domanda, e quindi entro il termine legale, soltanto in quattro casi (7%).

Il superamento del termine è stato spesso causato dall'assenza delle persone o delle autorità interessate (vacanze, malattia, viaggi di servizio), dal numero elevato di terzi coinvolti nella procedura o dalla complessità delle questioni giuridiche trattate. Questi motivi valgono anche per quei nove casi il cui trattamento ha superato i 100 giorni. Inoltre, rispettare i

Tabella 2: tempo di elaborazione delle procedure di mediazione

Tempo di elaborazione in giorni	Periodo 2014 - agosto 2016	Fase pilota 2017	Periodo 2018	Periodo 2019	Periodo 2020	Periodo 2021
entro 30 giorni	11%	59%	50%	57%	43%	42%
da 31 a 99 giorni	45%	37%	50%	38%	30%	51%
100 giorni o più	44%	04%	00%	05%	27%	7%

*Fonte: presentazione dell'Incaricato, evento per i dieci anni della LTras, 2 settembre 2016

termini è stato reso ancora più difficile a causa di consultazioni all'estero, di molteplici tentativi di mediazione tra le parti e della quantità di documenti o persone coinvolte. Poiché in questi casi il trattamento è spesso particolarmente dispendioso, secondo l'articolo 12^a dell'ordinanza sulla trasparenza (OTras; RS 152.31) l'Incaricato è libero di concedere una proroga ragionevole del termine ordinario.

Il legislatore ha concepito la mediazione come una procedura informale e non pregiudiziale intesa a comporre amichevolmente le controversie. L'esperienza mostra invece che quando i richiedenti o i terzi consultati coinvolgono una rappresentanza legale sin-

dalla procedura di accesso e poi di mediazione ciò non favorisce una soluzione semplice, pragmatica e rapida.

Mentre superamenti del breve termine di 30 giorni in casi complessi o in procedure con più parti coinvolte (ossia con più terzi interessati) sono considerati insiti nella struttura stessa del sistema a causa delle possibilità legali di proroga, i ritardi che continuano ad accumularsi, e che si spiegano unicamente con la mancanza di risorse umane disponibili, rappresentano dal profilo giuridico casi di giustizia ritardata.

Numero di casi pendenti

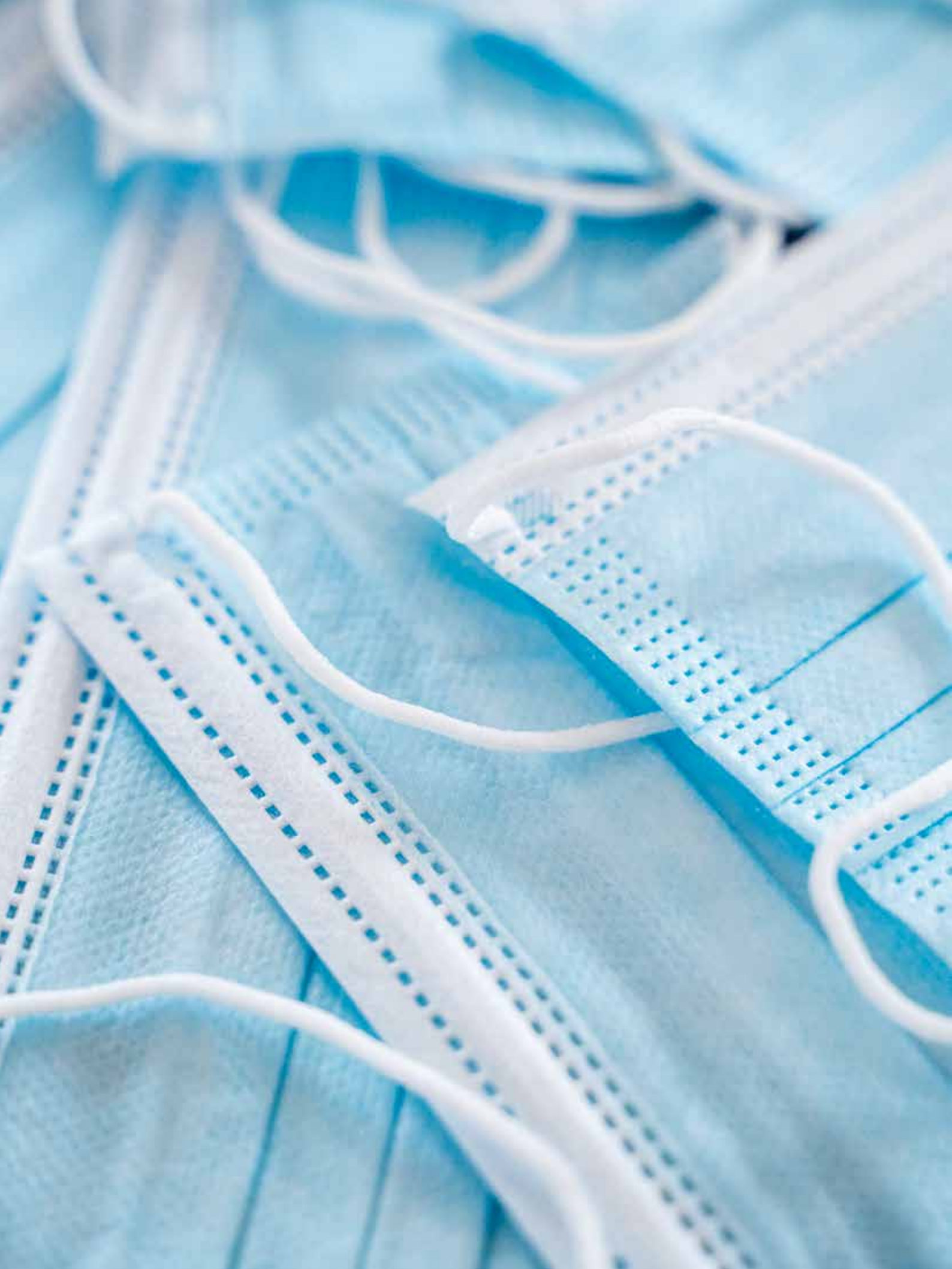
I dati riportati di seguito (Tab. 3) forniscono informazioni sul numero di casi pendenti alla fine dei rispettivi anni in rassegna. A fine 2021 erano pendenti 27 procedure di mediazione, di cui otto sospese (tre risalenti al 2019, una al 2020 e quattro all'anno in rassegna).

14 di questi casi hanno potuto essere conclusi entro la chiusura di redazione del presente rapporto.

È probabile che la durata di elaborazione aumenterà ancora, che vi sarà un'ulteriore crescita di sorpassi del termine ordinario non giustificabili dal profilo giuridico e che anche il numero dei casi pendenti alla fine del prossimo anno continuerà a salire.

Tabella 3: procedure di mediazione pendenti

Fine 2021	27 (di cui 14 evase entro la chiusura di redazione e 8 sospese)
Fine 2020	17 (di cui 9 evase entro la chiusura di redazione e 8 sospese)
Fine 2019	43 (di cui 40 evase entro la chiusura di redazione e 3 sospese)
Fine 2018	15 (di cui 13 evase nel febbraio 2019 e 2 sospese)



2.4 Procedura legislativa

CONSULTAZIONE DEGLI UFFICI

Revisione della legge federale sulle attività informative

La legge federale del 25 settembre 2015 sulle attività informative (LAI; RS 121) è attualmente in corso di revisione. Il progetto di revisione trasmesso all'Incaricato nell'ambito della consultazione degli uffici prevedeva una nuova estensione del campo delle informazioni escluse dalla legge sulla trasparenza.

In applicazione dell'attuale articolo 67 LAIn, la legge sulla trasparenza non si applica all'accesso a documenti ufficiali riguardanti l'acquisizione di informazioni secondo la LAIn. Questa nozione è chiaramente delimitata dal capitolo 3 della legge sulle attività informative. La nuova versione dell'articolo prevede ora di escludere tutti i dati sulle informazioni. Secondo l'Incaricato, modificando questa disposizione il Servizio

delle attività informative della Confederazione (SIC) tenta ancora una volta di limitare la portata della legge sulla trasparenza estendendo il campo delle informazioni escluse da essa. Con la nuova formulazione la maggior parte dell'attività del SIC non rientrerà nel campo d'applicazione della legge sulla trasparenza, cosa che andrebbe contro la volontà del legislatore che ha introdotto la suddetta legge per promuovere la trasparenza sulle attribuzioni, l'organizzazione e l'attività dell'amministrazione.

L'Incaricato vi si è fermamente opposto poiché, tra l'altro, le eccezioni previste agli articoli 7-9 LTras – in particolare quelle che consentono di proteggere la sicurezza interna o esterna della Svizzera (art. 7 cpv. 1 lett. c LTras), gli interessi della politica estera della Svizzera (art. 7 cpv. 1 lett. d LTras) e i dati personali (art. 7 cpv. 2 LTras) – trovano già applicazione e offrono una protezione sufficiente e adeguata.

A conclusione della consultazione degli uffici il SIC, dopo aver mantenuto inizialmente la propria posizione, ha infine informato l'Incaricato che avrebbe abbandonato la modifica dell'attuale articolo 67 LAIn.

L'IFPDT

3.1 Compiti e risorse

Pandemie

I progetti di trattamento di dati nella lotta alla pandemia, realizzati a breve termine a causa della crisi sanitaria, e la maggiore richiesta di documenti pubblici hanno sollecitato i collaboratori in modo straordinario anche nel secondo anno di pandemia.

In quanto unità della Confederazione, aggregata sul piano amministrativo alla Cancelleria federale, l'IFPDT ha attuato tutte le prescrizioni del Consiglio federale volte a proteggere la salute del personale. Dopo che, nel febbraio 2022, il Consiglio federale ha abolito l'obbligo generalizzato del telelavoro per il personale della Confederazione, dal 1° marzo 2022 il personale dell'IFPDT ha potuto ridurre il telelavoro conformemente al modello di lavoro flessibile ordinario concordato. Da allora gli incontri personali si sono intensificati, esplicando un effetto positivo in particolare sull'introduzione e il sostegno ai nuovi dipendenti.

Prestazioni e risorse nell'ambito della protezione dei dati

Effettivi del personale

Tra il 2005 e il 2019 l'effettivo del personale per l'esecuzione della legge federale sulla protezione dei dati (LPD) ha conosciuto una fluttuazione di 20-24 posti a tempo pieno. Le oscillazioni si spiegano da un lato con l'entrata in vigore della legge sulla trasparenza (LTras) nel 2006. Visto che i

posti previsti a tal fine non sono mai stati autorizzati dal Consiglio federale, la nostra autorità ha dovuto far capo al personale già esistente presso l'IFPDT e, in parte, alle risorse della Cancelleria federale. Dall'altro lato, per motivi di risparmio generali non è stato possibile reclutare tutto il personale destinato ai posti supplementari autorizzati nel contesto dell'adesione all'Accordo di Schengen e Dublino e dell'emanazione di leggi speciali nel settore sanitario.

Nel suo messaggio concernente la revisione totale della LPD il Consiglio federale aveva prospettato all'IFPDT la creazione di risorse supplementari nella misura di 9-10 posti (FF 2017 6154). Nel frattempo, con la nuova legge sulla protezione dei dati in ambito Schengen (LPDS, RS 235.3), il legislatore federale ha anticipato un aspetto parziale della revisione totale della LPD. Dopo aver posto in vigore la nuova legge al 1° marzo 2019, il Consiglio federale ha assegnato all'IFPDT tre ulteriori posti per l'attuazione dei nuovi compiti e delle nuove competenze, di modo che dal 2020 l'effettivo del personale ammonta a 27 posti a tempo pieno. Considerato che l'entrata in vigore della LPD riveduta era prevista per il 2022, nella primavera del 2021

l'IFPDT ha proposto al Consiglio federale di autorizzare i rimanenti sei posti a tempo pieno, i quali sono stati approvati nell'ambito della valutazione complessiva delle risorse. Con l'entrata in vigore della nuova legislazione, il Consiglio federale trasmetterà alle Camere federali per decisione soltanto le nuove richieste di risorse dell'IFPDT.

In seguito a pensionamenti e ad altre partenze, la struttura demografica dell'autorità è ringiovanita negli ultimi anni, il che sgrava il credito per il personale.

Tabella 4: Posti attribuibili per trattare questioni riguardanti la LPD

2005	22
2010	23
2018	24
2019	24
2020	27
2021	27
2022	27

Prestazioni

Secondo il nuovo Modello di gestione dell'Amministrazione federale (NMG), i compiti dell'IFPDT in quanto autorità di protezione dei dati competente per gli organi federali e l'economia privata sono attribuiti ai quattro gruppi di prestazioni consulenza, vigilanza, informazione e legislazione. Nell'anno in rassegna, dal 1° aprile 2021 al 31 marzo 2022, le risorse di personale impiegate

presso l'IFPDT che potevano essere destinate alla protezione dei dati sono state ripartite nei gruppi summenzionati nel modo seguente:

Tabella 5: Servizi protezione dei dati

Consulenza a privati	22,1%	
Consulenza alla Confederazione	18,9%	
Collaborazione con i Cantoni	1,4%	
Collaborazione con autorità estere	13,4%	
Totale Consulenza		55,8%
Vigilanza	16,8%	
Certificazione	0,1%	
Registro delle collezioni di dati	0,4%	
Totale Vigilanza		17,3%
Informazione	13,1%	
Formazione/ Conferenze	3,1%	
Totale Informazione		16,2%
Legislazione	10,7%	
Totale Legislazione		10,7%
Totale Protezione dei dati		100,0%

Consulenza

Come illustrato nel capitolo iniziale «Sfide attuali», nel settore della consulenza l'IFPDT è confrontato a una continua crescita delle richieste derivante dalla necessità di accompagnare grandi progetti digitali. Nell'anno in rassegna, le risorse di personale impiegate nella consulenza ammontavano a circa il 56 per cento. Secondo il piano di controllo dell'IFPDT per il 2022,

l'accompagnamento a titolo di consulenza è in corso per sette grandi progetti. Sei di essi sono legati alla trasformazione digitale disposta dal Consiglio federale per l'Amministrazione federale, la quale cerca di recuperare il ritardo nella digitalizzazione lamentato dalla politica e dai media proprio in relazione alla lotta contro la pandemia.

Considerato che le risorse dell'IFPDT sono tuttora insufficienti per affrontare i rischi giuridici e tecnologici di una digitalizzazione che procede in modo dinamico, anche nel periodo in rassegna la nostra autorità non ha potuto soddisfare l'accresciuta richiesta di accompagnamento di progetti con la dovuta accuratezza e nei tempi auspicati. I tre team dell'ambito direzionale Protezione dei dati hanno risposto mediamente ogni mese a 48 richieste e segnalazioni di cittadini, inviando agli interessati una lettera standard che li informava sulle vie previste dalla procedura civile. Ciò causa un'incomprensione sempre più grande poiché, da un lato, il Regolamento generale dell'UE sulla protezione dei dati (GDPR) impone alle proprie autorità di protezione dei dati di dare seguito a tutte le denunce dei cittadini e, dall'altro, la nuova LPD prevede anche per l'IFPDT un obbligo esteso di trattare sotto il profilo materiale singole istanze della popolazione svizzera.

Dato che i big data e l'intelligenza artificiale si stanno imponendo come modello aziendale in tutti i settori e i rischi tecnologici legati alla protezione dei dati continuano ad estendere il campo di vigilanza dell'IFPDT, il numero di grandi progetti pubblici e privati che implicano un trattamento di dati continuerà verosimilmente a crescere, come negli scorsi anni.

Tabella 6: Consulenze svolte nel 2021 per grandi progetti

Sanità e lavoro	3
Commercio e economia	3
Dogana	1
Totale	7

Vigilanza

La dinamica delle applicazioni basate su cloud impone oggi un'esecuzione estremamente rapida dei controlli. Questa accelerazione e la necessità, che si rivela sempre più importante, di disporre di una combinazione di conoscenze giuridiche e competenze tecniche escludono interruzioni prolungate nelle procedure di accertamento dei fatti, cosicché i controlli più estesi devono essere svolti da più collaboratori. L'attuale entità degli effettivi limita considerevolmente la densità dei controlli. Nel 2018 all'attività di vigilanza è stato attribuito più o meno il 12 per cento delle risorse di personale, quota sensibilmente inferiore al 20 per cento della media degli anni precedenti. Negli ultimi periodi in rassegna si è almeno potuto evitare che la quota scendesse sotto il 15 per cento. Nel periodo in rassegna essa era pari al 17,3 per cento, ossia circa due punti percentuali al

di sopra di tale valore di riferimento. Secondo il piano di controllo per il 2022, queste risorse dovranno servire a svolgere 13 controlli su vasta scala. Se rapportata al volume dei trattamenti di dati da parte di organi federali e alle circa 12 000 grandi e medie imprese commerciali nonché alle circa 100 000 fondazioni e associazioni attive in Svizzera, l'attuale densità dei controlli si rivela ancora bassa. Per l'Incaricato rimane dunque difficile far comprendere ai media e alle organizzazioni attive nella protezione dei consumatori le proprie reticenze, imputabili alla limitatezza delle risorse disponibili, ad avviare procedure formali per l'accertamento dei fatti. In vista dell'imminente entrata in vigore della nuova LPD l'aspettativa del pubblico è aumentata.

Legislazione

Gli adeguamenti del trattamento dei dati personali conseguenti alla trasformazione digitale degli uffici federali risultano leciti soltanto se si fondano su una base legale. Quest'ultima comporta l'introduzione nel diritto federale di tutta una serie di prescrizioni nuove e rivedute sul trattamento dei dati, in merito alle quali l'IFPDT si esprime nell'ambito delle diverse procedure di consultazione. Nonostante il corrispondente onere e la dispendiosa revisione della LPD e della relativa ordinanza, negli ultimi periodi in rassegna siamo riusciti a stabilizzare l'attività di vigilanza a un livello basso. Tuttavia, questo obiettivo è realizzabile soltanto limitando le analisi e i pareri dettagliati ai progetti chiave.

Revisione totale della legge sulla protezione dei dati

Con l'imminente entrata in vigore della nuova LPD e dell'ordinanza d'esecuzione, per l'IFPDT si prospettano onerosi lavori preparatori per quanto concerne i nuovi compiti e le nuove competenze come pure l'informazione tempestiva della popolazione e dell'economia. Grazie alla liberazione di tre posti da parte del Consiglio federale, avvenuta in vista dell'entrata in vigore della LPD, è stato possibile portare avanti tali lavori. A questo proposito, il Consiglio federale ha approvato anche gli ulteriori sei posti per l'attuazione della LPD (cfr. sopra).

Partecipazione a deliberazioni delle commissioni e audizioni da parte di commissioni parlamentari

- Nel periodo in rassegna, nell'aprile 2021 la CIP-N ci ha invitati a uno scambio sul tema delle agevolazioni COVID per persone vaccinate. Nello stesso mese la CTT-N ci ha consultati in merito alla revisione della LSCPT.

- A fine ottobre 2021 e a metà gennaio 2022 la CIP-N e la CIP-S ci hanno invitati tre volte a uno scambio sulla revisione della legge sulla protezione dei dati e delle relative ordinanze di esecuzione.
- Sempre nel mese di ottobre siamo stati sentiti dalla DelCG sulla presentazione di un rapporto sulla nostra prassi in merito all'articolo 64 LAIn.
- Nel novembre 2021 siamo stati inoltre sentiti dalla CIP-N in merito al preventivo 2022 e al piano finanziario 2023-2025.
- Alla fine del periodo in rassegna siamo stati consultati due volte dalla CSSS-S sulla problematica Swiss-transplant.
- Nel febbraio 2022, infine, la sotto-commissione DFGP/CaF della CdG-N ha effettuato una visita di servizio di mezza giornata, che si è svolta nei locali di Palazzo federale a causa della pandemia.

Criteri di valutazione

La responsabilità di decidere se e in che misura attribuire all'IFPDT risorse supplementari compete alle autorità politiche, che dispongono di un considerevole margine di manovra nel valutare gli sviluppi attuali e futuri della digitalizzazione e le sue ripercussioni sull'attività della nostra autorità. Il compito principale dell'IFPDT è proteggere la sfera privata e garantire il diritto all'autodeterminazione informativa nella società digitale. L'IFPDT deve poter agire in piena indipendenza.

Ciò richiede un'adeguata e sufficiente dotazione di risorse umane, materiali, tecniche e finanziarie, in modo che l'autorità di vigilanza non debba limitarsi a sbrigare l'indispensabile semplicemente reagendo, ma sia in grado di agire di sua iniziativa, in particolare con quella credibilità e quell'intensità che i cittadini possono ragionevolmente aspettarsi per la tutela dei loro diritti fondamentali.

Prestazioni e risorse nell'ambito della legge sulla trasparenza

L'anno in rassegna è stato caratterizzato non soltanto dalla pandemia, bensì in particolare dal significativo aumento delle richieste di mediazione (cfr. n. 2.2). A tal proposito è emerso nuovamente

che i 4,4 posti assegnati all'ambito direzionale Principio di trasparenza non sono sufficienti per adempiere i compiti conformemente alla legge. Come già menzionato – e contrariamente alle dichiarazioni contenute nel suo messaggio – il Consiglio federale non ha finora autorizzato alcun posto all'IFPDT per far fronte ai suoi compiti derivanti dalla legge sulla trasparenza.

A seguito della pandemia e delle misure adottate dal Consiglio federale per proteggere la salute pubblica, sia nell'anno in rassegna che nell'anno in corso non è nuovamente stato possibile, per diversi mesi, svolgere sul posto le procedure di mediazione. Di conseguenza, in tali periodi l'Incaricato è ritornato a svolgere le procedure per scritto: un fatto che ha avuto un impatto negativo sui tempi di elaborazione delle singole procedure e che ha causato un accumulo di procedure inevase. Inoltre, il numero da anni in costante aumento delle domande di mediazione e la loro crescente complessità hanno comportato che l'Incaricato

superasse il termine legale di trattazione di 30 giorni in una percentuale crescente di procedure.

La tendenza all'aumento di domande di mediazione sembra confermarsi anche per il 2022 e oltre facendo sì che l'accumulo di domande inevase renderà ulteriormente difficile trattare i nuovi casi entro i termini prescritti con le risorse attualmente disponibili. Non è quindi più garantita la rapida evasione delle procedure prevista dal legislatore.

Sempre in base al principio di trasparenza, spetta alle autorità politiche decidere se e in qual misura attribuire risorse all'IFPDT per adempiere i suoi compiti di mediazione e consulenza.

Per quanto riguarda i diversi gruppi di prestazioni, la valutazione delle risorse deve fondarsi sui seguenti obiettivi di efficacia:

Tabella 7: Criteri di quantificazione IFPDT

Gruppo di prestazioni	Obiettivi di efficacia
Consulenza	L'IFPDT dispiega una presenza conforme alle attese per la consulenza a privati e per il monitoraggio di progetti sensibili in materia di protezione dei dati dell'economia e delle autorità federali, avvalendosi di strumenti di lavoro adeguati alla realtà digitale.
Vigilanza	L'IFPDT dispiega una densità di controlli credibile.
Informazione	L'IFPDT sensibilizza l'opinione pubblica in modo proattivo sui rischi legati alla tecnologia e alle applicazioni nel contesto della digitalizzazione. Dispone di un sito Internet moderno e di facile consultazione. Le notifiche dovranno poter essere recapitate all'IFPDT in modo sicuro, semplice e in qualsiasi momento per il tramite di portali di notifica.
Legislazione	L'IFPDT esercita attivamente e tempestivamente la propria influenza nell'elaborazione di tutte le norme speciali e di tutti i regolamenti che hanno un impatto in materia di protezione dei dati, a livello nazionale e internazionale. Sostiene le cerchie interessate nella formulazione di regole di buona prassi.

3.2 Comunicazione

Principali temi dell'attività di comunicazione

I temi legati alla pandemia che già avevano dominato il periodo precedente hanno continuato a essere presenti anche nell'anno in rassegna. Tuttavia, le domande rivolte all'IFPDT si sono concentrate meno sul tracciamento dei contatti (contact tracing) e più sulla concezione e sull'impiego del certificato COVID-19 e sulla sua App. L'Incaricato e i suoi esperti hanno continuato a essere sollecitati al riguardo dal punto di vista della comunicazione. Ci siamo impegnati con successo a favore del certificato light, una versione contenente solo i dati indispensabili e in cui non sono memorizzati dati sanitari. C'è poi stata la questione della piattaforma di registrazione delle vaccinazioni *lemievaccinazioni.ch*, il cui gestore ha chiuso il portale a causa di falle a livello di sicurezza. Gran parte dell'attività di comunicazione ha riguardato temi legati al coronavirus.

Altro importante tema sono state le fughe di dati in vari settori, spesso scoperte da reti di giornalisti investigativi. Sono state colpite sia reti sociali

sia piattaforme con un elevato interesse pubblico, per esempio quelle del trasporto pubblico, della donazione di organi o delle protesi mammarie. Abbiamo inoltre ricevuto molte segnalazioni di attacchi a sistemi aziendali. Di conseguenza, abbiamo intensificato i nostri scambi con il Centro nazionale per la cibersicurezza (NCSC). Le avvenute fughe di dati devono essere obbligatoriamente notificate all'IFPDT soltanto a partire da quando entrerà in vigore la nuova legge federale sulla protezione dei dati (cfr. tema prioritario I).

Abbiamo continuato a concentrarci sulla vigilanza – sia nel settore lavorativo, nei settori privati come il commercio al dettaglio o tramite software di spionaggio dello Stato. Il tracciamento (comportamento in fatto di mobilità, di utilizzo di Internet o di consumo) e lo sviluppo di sistemi di riconoscimento biometrico che utilizzano algoritmi per spiare la popolazione (p. es. Clearview), continuano a essere ambiti dinamici che hanno suscitato l'interesse dei media e continueranno a farlo. Le questioni relative alla protezione dei dati rimangono essenziali in numerosi progetti di trasformazione digitale dell'Amministrazione federale e dell'economia privata.

Nell'anno in rassegna il settore Comunicazione dell'IFPDT e l'Incaricato hanno trattato in totale 550 richieste provenienti da media e altre organizzazioni.

Crescente attenzione da parte dei media e della popolazione

Nel nostro monitoraggio dei media, basato su una selezione di media svizzeri e prodotti chiave della stampa internazionale, abbiamo registrato oltre 6000 contributi rispetto ai 4000 dell'anno precedente. Si conferma dunque la tendenza già constatata secondo cui l'attenzione nei confronti della protezione dei dati e dell'autodeterminazione informativa continua a crescere e si riflette in una corrispondente copertura mediatica più ampia. Nel complesso, nei media si è osservato un leggero calo della presenza di temi legati al coronavirus che hanno rappresentato ancora circa un terzo degli articoli osservati. I giornalisti si sono inoltre concentrati su temi legati alla vigilanza, alla trasmissione dei dati e alle questioni normative riguardanti i colossi tecnologici (GAFAM), i settori cloud, cibersicurezza o intelligenza artificiale e big data.

Si nota anche un aumento dei rapporti fondati su documenti che hanno potuto essere ottenuti in base alla legge sulla trasparenza.

Sono aumentate anche le domande e le richieste che la nostra autorità ha ricevuto dalla popolazione e dalle imprese. Abbiamo trattato circa 6600 domande per e-mail, per posta oppure attraverso la linea diretta telefonica (lo scorso anno erano state 4200).

L'Incaricato ha partecipato a una cinquantina di eventi, quindi un po' più dell'anno precedente. Durante la Giornata internazionale della protezione dei dati, che si è svolta a fine gennaio 2022, ha partecipato alla conferenza pubblica dell'Università di Losanna. Nel suo intervento l'Incaricato ha sottolineato che le autorità preposte alla protezione dei dati hanno lavorato affinché la trasformazione digitale possa procedere nel rispetto del diritto fondamentale a una vita privata e auto-determinata.

Rapporto d'attività e sviluppo di un nuovo sito Internet

Alla fine dell'anno in rassegna il settore Comunicazione è composto da tre collaboratori per un totale di 2,6 posti a tempo pieno. Pure il lavoro mediatico ha la priorità come il progetto del rapporto d'attività annuale. Il 28° rapporto d'attività 2020/21 previsto dall'articolo 30 LPD è stato pubblicato il 29 giugno 2021. Il documento è stato prodotto

e stampato nuovamente in quattro lingue. Il rapporto può essere inoltre visionato sul nostro sito Internet nel formato accessibile e-paper oppure nel tradizionale formato PDF.

Nell'autunno del 2021 ai nostri temi prioritari abbiamo aggiunto lo sviluppo del nuovo sito Internet. In seguito a una procedura mediante invito, nel 2022 abbiamo potuto dare il via alla fase concettuale con l'aiuto di un'agenzia esterna. L'obiettivo è quello di semplificare una struttura formatasi nel corso di molti anni e di aggiornare il contenuto in modo che gli utenti possano utilizzare un sito Internet moderno, di facile impiego e adatto alle loro esigenze. Il nuovo sito Internet dell'IFPDT terrà conto delle disposizioni della nuova legge sulla protezione dei dati e sarà lanciato prima dell'entrata in vigore del nuovo testo normativo.

Pareri e raccomandazioni

Nell'anno in rassegna l'Incaricato ha pubblicato diversi pareri e dichiarazioni su progetti ed eventi d'attualità, riguardanti tra l'altro i seguenti temi:

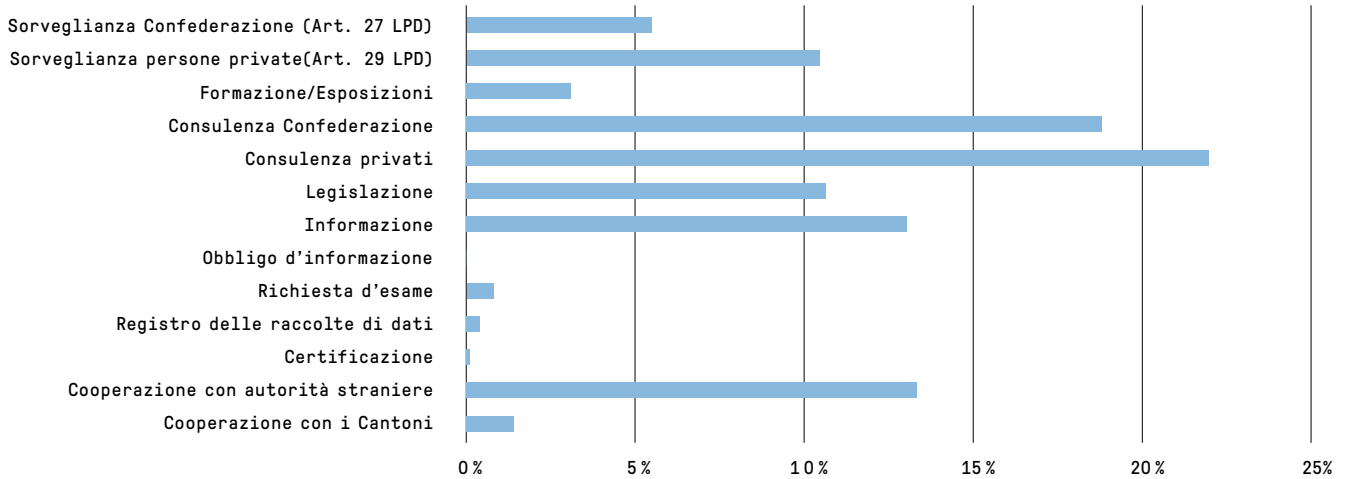
- Accertamenti dei fatti sull'applicazione SocialPass e sulle piattaforme «lemievaccinazioni.ch» e Swiss-transplant
- Sorveglianza di persone presunta e non autorizzata (Mitto AG)
- Accompagnamento del certificato vaccinale COVID e della versione light, contenente solo i dati indispensabili
- Trasmissione di dati all'estero
- Trasmissione di dati non conforme alla LPD presso la società svizzera dei tiratori
- Diverse fughe di dati tra l'altro anche sulle reti sociali

Sul nostro sito Internet abbiamo pubblicato 45 raccomandazioni riguardanti l'accesso a documenti amministrativi in base al principio di trasparenza (contro le 26 nel 2020).

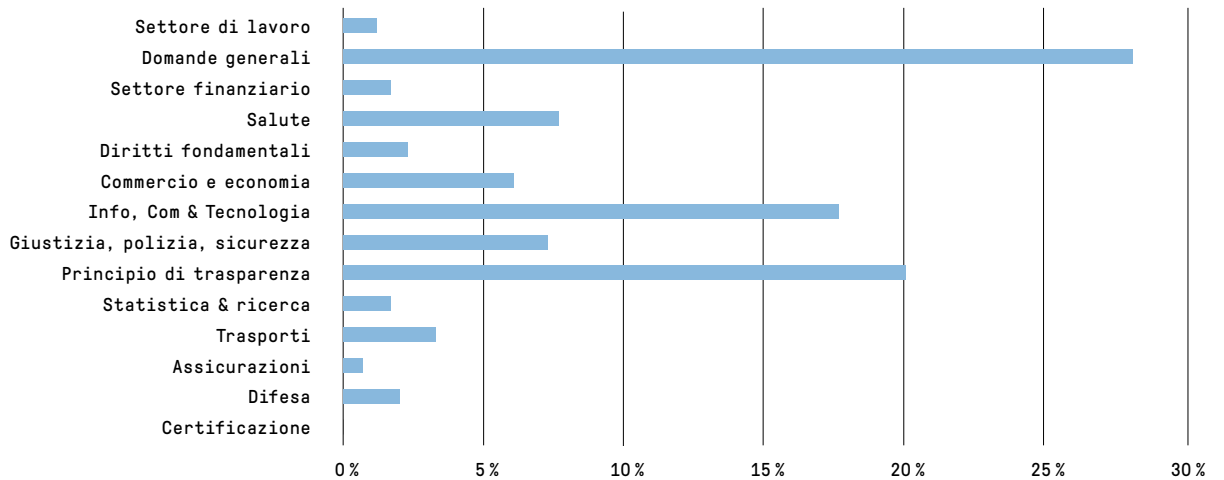
3.3 Statistiche

Statistiche sulle attività dell'IFPDT dal 1° aprile 2021 al 31 marzo 2022 (Protezione dei dati)

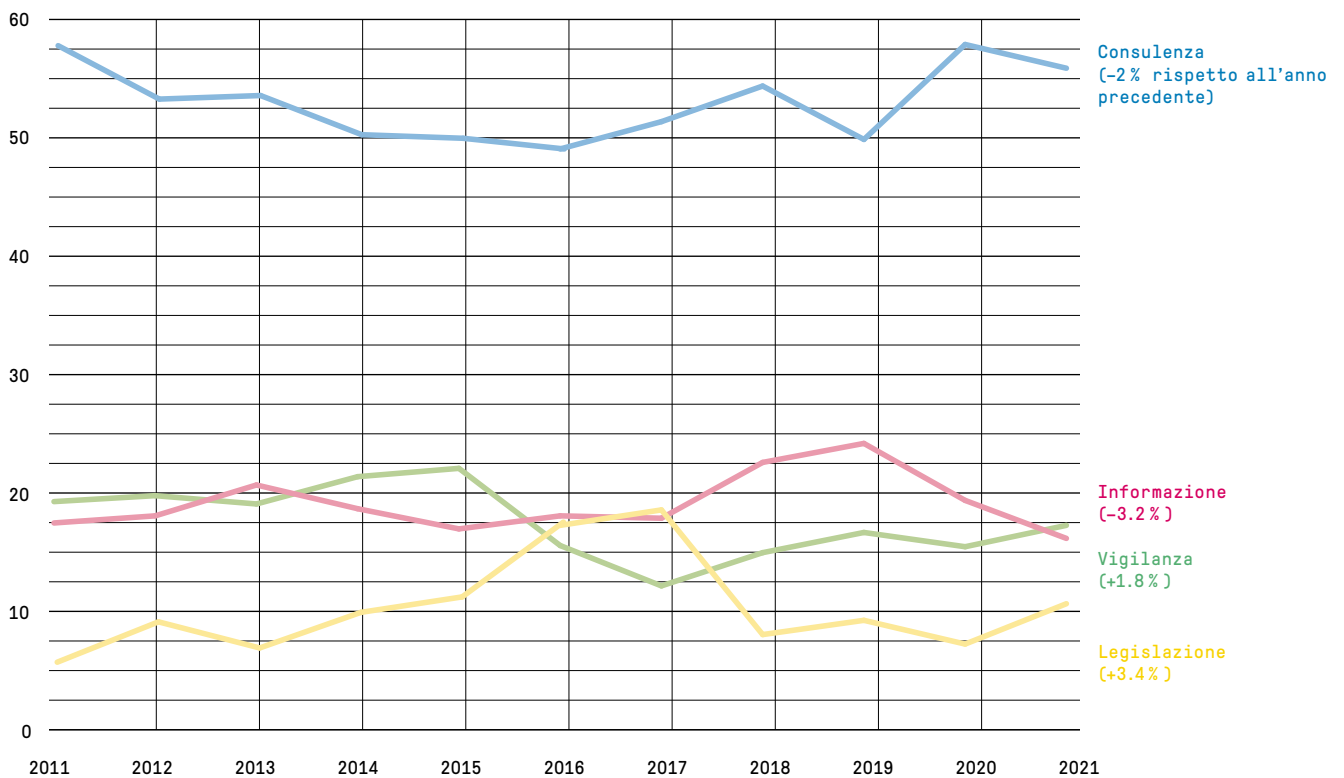
Carico di lavoro per compiti



Carico di lavoro per materie



Paragone pluriennale (in percentuale)



Panoramica delle domande d'accesso dal 1° gennaio al 31 dicembre 2021

Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
CaF	57	26	8	9	2	5	7
DFAE	156	77	15	47	2	5	10
DFI	422	168	25	139	21	38	31
DFGP	103	46	18	13	1	2	23
DDPS	281	203	11	38	7	3	19
DFF	119	54	22	21	6	9	7
DEFR	92	48	13	22	2	6	1
DATEC	146	71	10	35	6	10	14
MPC	8	0	4	0	1	0	3
SP	1	1	0	0	0	0	0
Totale 2021 (%)	1385 (100)	694 (50)	126 (9)	324 (23)	48 (3)	78 (7)	115 (8)
Totale 2020 (%)	1193 (100)	610 (51)	108 (9)	293 (24)	35 (3)	80 (7)	67 (6)
Totale 2019 (%)	916 (100)	542 (59)	86 (9)	171 (19)	38 (4)	43 (5)	36 (4)
Totale 2018 (%)	647 (100)	355 (55)	66 (10)	119 (18)	24 (4)	50 (8)	33 (5)
Totale 2017 (%)	586 (100)	325 (56)	108 (18)	106 (18)	21 (4)	26 (4)	-
Totale 2016 (%)	558 (100)	299 (54)	88 (16)	105 (19)	29 (5)	33 (6)	-
Totale 2015 (%)	600 (100)	320 (53)	99 (17)	128 (21)	31 (5)	22 (4)	-
Totale 2014 (%)	582 (100)	302 (52)	124 (21)	124 (21)	15 (3)	17 (3)	-
Totale 2013 (%)	461 (100)	218 (46)	123 (26)	103 (22)	18 (4)	8 (2)	-
Totale 2012 (%)	522 (100)	230 (44)	140 (27)	123 (24)	19 (4)	6 (1)	-
Totale 2011 (%)	481 (100)	206 (44)	127 (27)	128 (27)	0 (0)	9 (2)	-

**Statistica delle domande d'accesso secondo la legge sulla trasparenza
dal 1° gennaio al 31 dicembre 2021**

	Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	41	19	6	7	2	0	7
	IFPDT	16	7	2	2	0	5	0
	Totale	57	26	8	9	2	5	7
Dipartimento federale degli affari esteri DFAE	DFAE	156	77	15	47	2	5	10
	Totale	156	77	15	47	2	5	10
Dipartimento federale dell'interno DFI	SG DFI	13	8	0	2	0	2	1
	UFU	24	20	0	0	1	0	3
	UFC	1	0	1	0	0	0	0
	AFS	1	1	0	0	0	0	0
	METEO CH	0	0	0	0	0	0	0
	BN	0	0	0	0	0	0	0
	UFSP	251	90	11	101	6	27	16
	UST	12	8	3	0	0	0	1
	UFAS	13	8	3	1	0	0	1
	compenswiss	2	1	1	0	0	0	0
	USAV	28	17	1	9	1	0	0
	MNS	0	0	0	0	0	0	0
	SWISS MEDIC	72	15	3	26	11	8	9
	SUVA	5	0	2	0	2	1	0
	Totale	422	168	25	139	21	38	31
Dipartimento federale di giustizia e polizia DFGP	SG DFGP	14	7	0	1	0	1	5
	DFGP	38	13	10	0	0	0	15
	FEDPOL	14	10	3	1	0	0	0
	METAS	1	1	0	0	0	0	0
	SEM	24	10	2	9	1	0	2
	Servizio SCPT	3	0	0	2	0	0	1
	ISDC	5	2	3	0	0	0	0
	IPI	2	2	0	0	0	0	0
	CFCG	0	0	0	0	0	0	0
	CAF	1	1	0	0	0	0	0
	ASR	0	0	0	0	0	0	0
	CSI	0	0	0	0	0	0	0
	CNPT	1	0	0	0	0	1	0
	Totale	103	46	18	13	1	2	23

	Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	27	10	0	8	0	1	8
	Difesa	29	17	1	7	3	1	0
	SIC	28	0	6	15	0	0	7
	armasuisse	12	3	4	3	0	1	1
	UFSP0	172	170	0	0	2	0	0
	UFPP	8	1	0	5	0	0	2
	swisstopo	5	2	0	0	2	0	1
	UUC	0	0	0	0	0	0	0
	Totale	281	203	11	38	7	3	19
Dipartimento federale delle finanze DFF	SC DFF	25	8	6	7	0	2	2
	ODIC ¹⁾	0	0	0	0	0	0	0
	AFF	7	2	0	3	0	0	2
	UFPER	4	4	0	0	0	0	0
	AFC	14	4	7	3	0	0	0
	AFD ²⁾	42	22	3	7	4	6	0
	UFCL	5	3	1	0	1	0	0
	UFIT	7	5	0	0	1	0	1
	CDF	9	1	4	1	0	1	2
	¹⁾ Dal 1.1.2021 al CaF TDT	SFI	3	3	0	0	0	0
²⁾ Dal 1.1.2022 UDSC	PUBLICA	0	0	0	0	0	0	0
	UCC	3	2	1	0	0	0	0
	Totale	119	54	22	21	6	9	7

	Sezione	Numero di domande	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	6	6	0	0	0	0	0
	SECO	28	18	3	4	2	1	0
	SEFRI	13	10	2	0	0	0	1
	UFAG	13	3	1	8	0	1	0
	Agroscope	3	2	0	1	0	0	0
	UFAE	2	1	1	0	0	0	0
	UFAB	1	0	0	1	0	0	0
	SPR	4	1	3	0	0	0	0
	COMCO	10	4	1	3	0	2	0
	CIVI	0	0	0	0	0	0	0
	UFDC	1	0	0	0	0	1	0
	FNS	0	0	0	0	0	0	0
	IUFFP	1	0	1	0	0	0	0
	ETH Rat	9	2	1	5	0	1	0
	Innosuisse	1	1	0	0	0	0	0
Totale	92	48	13	22	2	6	1	
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	SG DATEC	12	8	1	0	0	1	2
	UFA	7	3	0	2	0	1	1
	UFAC	10	6	1	1	1	1	0
	UFE	11	3	3	3	0	1	1
	USTRA	6	5	0	1	0	0	0
	UFCOM	23	9	0	11	0	1	2
	UFAM	64	34	4	15	3	1	7
	ARE	0	0	0	0	0	0	0
	ComCom	0	0	0	0	0	0	0
	IFSN	9	2	0	1	2	3	1
	PostCom	3	1	0	1	0	1	0
	AIRR	1	0	1	0	0	0	0
	Totale	146	71	10	35	6	10	14
Ministero pubblico della Confederazione MPC	MPC	8	0	4	0	1	0	3
	Totale	8	0	4	0	1	0	3
Servizi del Parlamento SP	SP	1	1	0	0	0	0	0
	Totale	1	1	0	0	0	0	0
Somma totale	1385	694	126	324	48	78	115	

Domande di accesso 2021 con riferimento a Corona

Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Cancelleria federale CaF	CaF	5	3	1	1	0	0
	IFPDT	0	0	0	0	0	0
	Totale	5	3	1	1	0	0
Dipartimento federale degli affari esteri DFAE	DFAE	0	0	0	0	0	0
	Totale	0	0	0	0	0	0
Dipartimento federale dell'interno DFI	SG DFI	6	5	0	0	0	1
	UFU	0	0	0	0	0	0
	UFC	0	0	0	0	0	0
	AFS	0	0	0	0	0	0
	METEO CH	0	0	0	0	0	0
	BN	0	0	0	0	0	0
	UFSP	217	82	2	93	4	20
	UST	0	0	0	0	0	0
	UFAS	1	1	0	0	0	0
	compenswiss	0	0	0	0	0	0
	USAV	0	0	0	0	0	0
	MNS	0	0	0	0	0	0
	SWISS MEDIC	41	6	2	17	6	6
	SUVA	1	0	0	0	1	0
Totale	266	94	4	110	11	27	
Dipartimento federale delle finanze DFF	SC DFF	5	0	4	1	0	0
	ODIC ¹⁾	0	0	0	0	0	0
	AFF	6	1	0	3	0	0
	UFPER	0	0	0	0	0	0
	AFC	1	0	1	0	0	0
	AFD ²⁾	2	0	0	2	0	0
	UFCL	1	0	0	0	1	0
	UFIT	6	3	0	1	1	0
	CDF	1	0	0	0	0	1
	SFI	0	0	0	0	0	0
¹⁾ Dal 1.1.2021 al CaF TDT ²⁾ Dal 1.1.2022 UDSC	PUBLICA	0	0	0	0	0	0
	UCC	0	0	0	0	0	0
	Totale	22	4	5	7	2	1

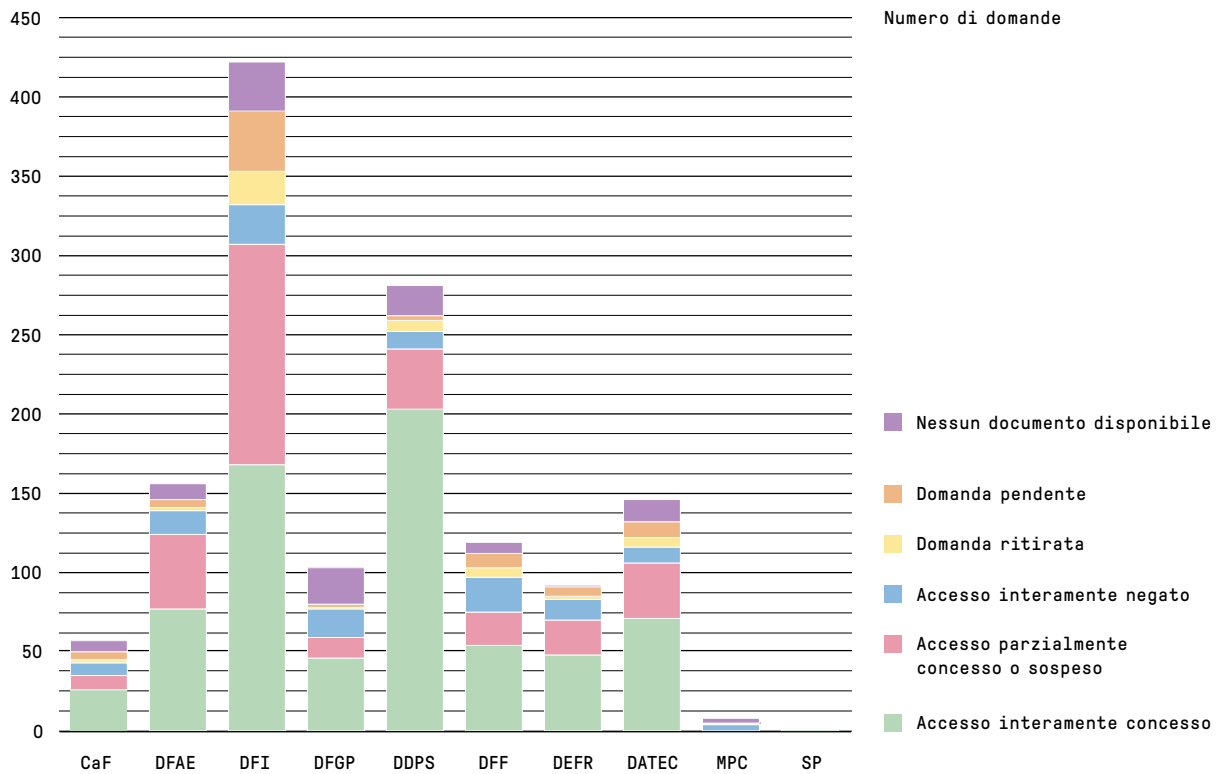
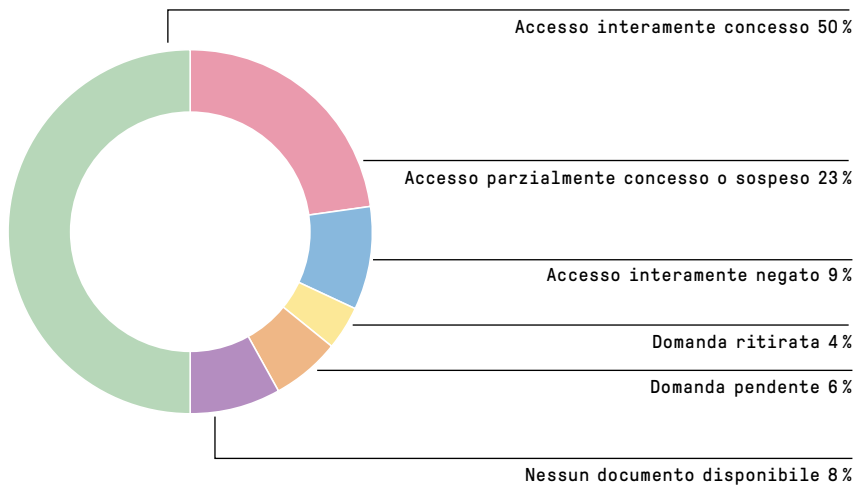
Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile	
Dipartimento federale di giustizia e polizia DFGP	SG DFGP	1	1	0	0	0	0	
	DFGP	0	0	0	0	0	0	
	FEDPOL	0	0	0	0	0	0	
	METAS	0	0	0	0	0	0	
	SEM	0	0	0	0	0	0	
	Servizio SCPT	0	0	0	0	0	0	
	ISDC	0	0	0	0	0	0	
	IPI	0	0	0	0	0	0	
	CFCG	0	0	0	0	0	0	
	CAF	0	0	0	0	0	0	
	ASR	0	0	0	0	0	0	
	CSI	0	0	0	0	0	0	
	CNPT	0	0	0	0	0	0	
	Totale	1	1	0	0	0	0	0
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC	SG DATEC	0	0	0	0	0	0	
	UFA	0	0	0	0	0	0	
	UFAC	1	0	0	1	0	0	
	UFE	0	0	0	0	0	0	
	USTRA	0	0	0	0	0	0	
	UFCOM	1	0	0	1	0	0	
	UFAM	0	0	0	0	0	0	
	ARE	0	0	0	0	0	0	
	ComCom	0	0	0	0	0	0	
	IFSN	0	0	0	0	0	0	
	PostCom	0	0	0	0	0	0	
	AIRR	0	0	0	0	0	0	
	Totale	2	0	0	2	0	0	0
	Département fédéral de la défense, de la protection de la population et des sports DDPS	SG DDPS	0	0	0	0	0	0
Difesa/ Esercito		25	15	1	5	3	1	
SIC		0	0	0	0	0	0	
armasuisse		0	0	0	0	0	0	
UFSP0		4	2	0	0	2	0	
UFPP		1	0	0	1	0	0	
swisstopo		0	0	0	0	0	0	
UUC		0	0	0	0	0	0	
Totale		30	17	1	6	5	1	0

Sezione	Domande con riferimento a Corona	Accesso interamente concesso	Accesso interamente negato	Accesso parzialmente concesso o sospeso	Domanda ritirata	Domanda pendente	Nessun documento disponibile
Dipartimento federale dell'economia, della formazione e della ricerca DEFR	SG DEFR	1	1	0	0	0	0
	SECO	5	1	1	3	0	0
	SEFRI	1	0	0	0	0	1
	UFAG	0	0	0	0	0	0
	Agroscope	0	0	0	0	0	0
	UFAE	0	0	0	0	0	0
	UFAB	0	0	0	0	0	0
	SPR	0	0	0	0	0	0
	COMCO	0	0	0	0	0	0
	CIVI	0	0	0	0	0	0
	UFDC	0	0	0	0	0	0
	FNS	0	0	0	0	0	0
	IUFFP	0	0	0	0	0	0
	ETH Rat	3	0	1	2	0	0
	Innosuisse	0	0	0	0	0	0
Totale	10	2	2	5	0	0	1
Ministero pubblico della Confederazione MPC	BA	0	0	0	0	0	0
	Total	0	0	0	0	0	0
Servizi del Parlamento SP	SP	0	0	0	0	0	0
	Totale	0	0	0	0	0	0
Somma totale	336	121	13	131	18	29	24

Numero di domande di mediazione secondo la categoria di richiedenti

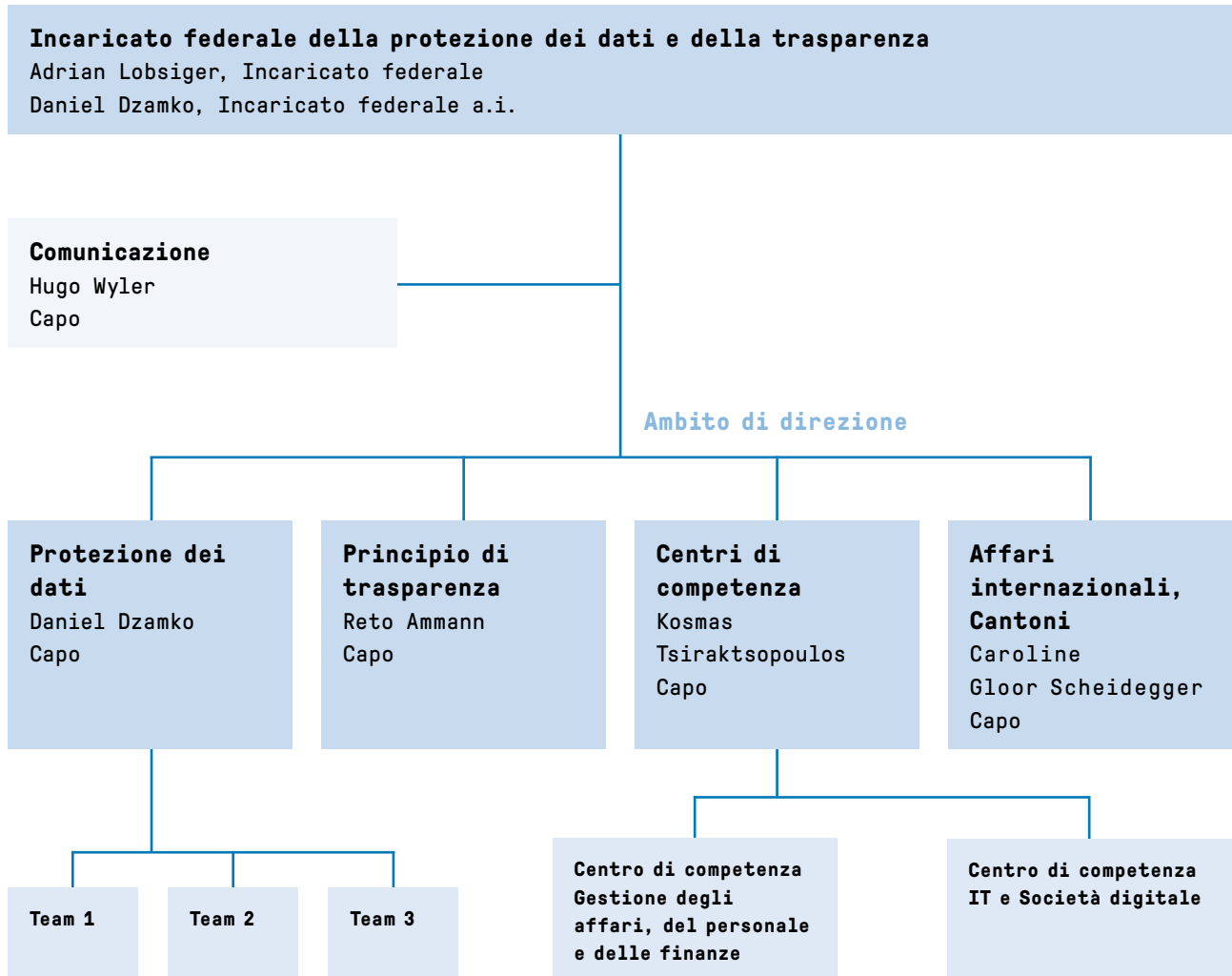
Categoria di richiedenti	2021	2020	2019	2018	2017
Media	53	31	34	24	21
Privati (o nessuna assegnazione esatta possibile)	49	42	40	26	35
Parti interessate (associazioni, organizzazioni, società ecc.)	16	5	7	9	14
Avvocati	12	7	5	4	2
Aziende	19	7	47	13	7
Università	0	1			
Totale	149	93	133	76	79

**Trattamento delle domande d'accesso
dal 1° gennaio al 31 dicembre 2021**



3.4 Organizzazione IFPDT (Stato 31 marzo 2022)

Organigramma



Personale dell'IFPDT

Numero di dipendenti	39		
FTE	32.4		
per sesso	Donne	19	49%
	Uomini	20	51%
per livello di occupazione	1-89%	27	69%
	90-100%	12	31%
per lingua	Tedesco	29	77%
	Francese	8	20%
	Italiano	1	3%
per età	20-49 anni	23	59%
	50-65 anni	16	41%
Posizioni dirigenziali	Donne	3	33%
	Uomini	6	67%

Abbreviazioni

AMVP Assemblea mondiale per la protezione della vita privata

CEPD Comitato europeo per la protezione dei dati

CGUE Corte di giustizia dell'Unione europea

CIP Cartella informatizzata del paziente

Convenzione 108+ Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

Datareg Registro delle collezioni di dati

DaziT Programma di trasformazione completa dell'UDSC

EDM Ente dei dati sulla mobilità

Fedpol Ufficio federale di polizia

GDPR Regolamento generale sulla protezione dei dati

GEPD Garante europeo della protezione dei dati

IA Intelligenza artificiale

le Identità elettronica

LCIP Legge federale sulla cartella informatizzata del paziente

LDP Legge federale sui diritti politici

LIDMo Legge federale sull'infrastruttura di dati sulla mobilità

LMeCA Legge federale concernente l'impiego di mezzi elettronici per l'adempimento dei compiti delle autorità

LDP Legge federale sulla protezione dei dati

LPDS Legge federale sulla protezione dei dati personali nell'ambito dell'applicazione dell'acquis di Schengen in materia penale

LSIe Legge federale sui servizi d'identificazione elettronica (legge sull'Ie)

LTras Legge federale sul principio di trasparenza dell'amministrazione (Legge sulla trasparenza)

LTV Legge sul trasporto di viaggiatori

NaDB Programma di gestione nazionale dei dati

NADIM Infrastruttura nazionale di dati sulla mobilità

NCSC Centro nazionale per la cibersicurezza

OCPD Ordinanza sulle certificazioni in materia di protezione dei dati

OCSE Organizzazione per la Cooperazione e lo Sviluppo Economico

OLPD Ordinanza relativa alla legge federale sulla protezione dei dati

PNR Dati dei passeggeri aerei (Passenger Name Records)

Privatim Conferenza degli incaricati svizzeri per la protezione dei dati

nLPD Nuova legge federale sulla protezione dei dati

SAS Servizio di accreditamento svizzero

SCC Clausole contrattuali standard

SEC Autorità di vigilanza del mercato finanziario

SIC Servizio delle attività informative della Confederazione

TDT Settore Trasformazione digitale e governance delle TIC della Cancelleria federale

TIC Tecnologie dell'informazione e della comunicazione

UDSC Ufficio federale della dogana e della sicurezza dei confini

Indice figurativo

Figure

Figura 1: Valutazione delle domande di accesso – Sviluppo dal 2008 p. 73

Figura 2: Tasse riscosse dall'entrata in vigore della LTras.....p. 75

Figura 3: Domande di mediazione dall'entrata in vigore della LTras p. 76

Tabelle

Tabella 1: Soluzioni consensualip. 77

Tabella 2: tempo di elaborazione delle procedure di mediazione..... p. 78

Tabella 3: procedure di mediazione pendenti p. 79

Tabella 4: Posti attribuibili per trattare questioni riguardanti la LPD..... p. 84

Tabella 5: Servizi protezione dei dati .. p. 85

Tabella 6: Consulenze svolte nel 2021 per grandi progetti p. 85

Tabella 7: Obiettivi di efficacia dell'IFPDTp. 87

Impressum

Il presente rapporto è disponibile in quattro lingue e anche in versione elettronica su Internet (www.lincaricato.ch).

Distribuzione: UFCL, Pubblicazioni federali, CH-3003 Berna

www.bundespublikationen.admin.ch

Art.-Nr. 410.029.I

Layout: Ast & Fischer AG, Wabern

Fotografia: Tim Troxler

Caratteri: Pressura, Documenta

Stampa: Ast & Fischer AG, Wabern

Carta: PlanoArt®, holzfrei hochweiss



Cifre chiave

Carico protezione dei dati

55,8%

Consulenza

17,3%

Vigilanza

16,2%

Informazione

10,7%

Legislazione

Domande d'accesso principio di trasparenza (LTras)

50%

interamente
concesso

23%

parzialmente
concesso o sospeso

9%

interamente
negato

4%

ritirata

6%

pendente

8%

nessun documento
disponibile

Preoccupazioni relative alla protezione dei dati



Informazione corretta

Le aziende e gli organi federali forniscono informazioni trasparenti sul loro trattamento dei dati: comprensibili e complete.



Possibilità di scelta

Gli interessati danno il loro consenso e godono di una vera libertà di scelta.



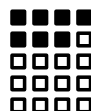
Analisi dei rischi

I possibili rischi per la protezione dei dati sono già stati identificati nel progetto e i loro effetti sono stati minimizzati con misure adeguate.



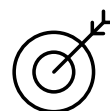
Esattezza dei dati

Il trattamento avviene con i dati corretti.



Proporzionalità

Nessuna raccolta di dati a conservazione, ma solo nella misura necessaria per raggiungere lo scopo. Il trattamento dei dati è limitato nel tempo e nella portata.



Finalità

I dati vengono trattati esclusivamente per le finalità indicate al momento della raccolta, come indicato dalle circostanze o come previsto dalla legge.



Sicurezza dei dati

I responsabili del trattamento garantiscono con misure tecniche e organizzative che i dati personali sono adeguatamente protetti.



Documentazione

Tutti i trattamenti sono documentati e classificati dal responsabile del trattamento.



Responsabilità personale

Gli organi privati e federali sono responsabili dell'adempimento dell'obbligo di rispettare la legislazione in materia di protezione dei dati.

Incaricato federale della protezione dei dati e della trasparenza
Feldeggweg 1
CH-3003 Berna

E-Mail: info@edoeb.admin.ch

Sito web: www.lincaricato.ch

🐦 @derBeauftragte

Telefono: +41 (0)58 462 43 95 (lu-ve, 10-12)

Fax: +41 (0)58 465 99 96