Messaggio

numero	data	competenza
8281	17 maggio 2023	CANCELLERIA DELLO STATO

Revisione totale della legge cantonale sulla protezione dei dati personali

Signora Presidente,
signore e signori deputati,

con il presente messaggio, ci pregiamo sottoporre al vostro esame le proposte per l'adozione di una nuova legge cantonale sulla protezione dei dati personali.

I. INTRODUZIONE

Il contesto tecnologico e sociale attuale è caratterizzato da forti dinamiche evolutive e da altrettanto forti effetti erosivi sui diritti e sulle libertà (nel settore pubblico, si pensi in particolare alla sorveglianza pubblica e al rischio di monitoraggio completo della persona, al tracciamento dettagliato dei consumi di energia elettrica e di acqua potabile, alla centralizzazione e alla condivisione di dati, all'interconnessione di banche dati con allestimento di profili della personalità, al rischio di pirateria informatica nei confronti di dati pubblici, alle decisioni basate esclusivamente su elaborazioni automatizzate di dati personali). I conseguenti cambiamenti legislativi internazionali in ambito di protezione dei dati a monte della presente revisione perseguono scopi tanto ambiziosi quanto difficili e, per certi versi, antitetici: garantire e rafforzare, da un lato, la tutela dei diritti e delle libertà fondamentali delle persone rispetto alle attività di trattamento dei dati personali. Dall'altro, si vogliono ottimizzare i flussi internazionali di dati, rispettivamente la libera circolazione dei dati, contribuendo in particolare al progresso dell'economia digitale. In pratica, secondo la nuova impostazione internazionale, le trasformazioni economiche indotte dalle nuove tecnologie vanno mantenute e incentivate, garantendo nel contempo il necessario clima di fiducia e la necessaria sicurezza giuridica grazie a un'elevata e coerente protezione dei dati personali, livellata sullo stesso piano d'equivalenza per tutti gli organi responsabili della protezione dei dati.

Ciò ha richiesto la costruzione di un quadro giuridico internazionale, nazionale e cantonale più solido e coerente in materia di protezione dei dati personali, affiancato da efficaci misure di attuazione.

Il diritto nazionale e cantonale sulla protezione dei dati non garantisce più un livello di protezione adeguato e va quindi modernizzato, tenendo conto delle riforme del diritto superiore. La Svizzera non è tenuta a recepire integralmente il nuovo diritto internazionale, ma deve garantire l'adeguatezza del proprio diritto interno con il diritto superiore. Se, in occasione della sua prossima valutazione, la Commissione europea dovesse arrivare alla conclusione che la legislazione svizzera non offre più un livello di protezione dei dati adeguato, potrà revocare, modificare o sospendere l'attuale decisione di adeguatezza.

L'economia, in particolare le piccole e medie imprese, potrebbero essere penalizzate, dovendo esse garantire la protezione dei dati nell'ambito del commercio con l'Unione europea in altro modo, ad esempio tramite contratti ad hoc con le aziende e la clientela dell'Unione europea. La stessa cooperazione giudiziaria in materia penale e di polizia potrebbe essere compromessa qualora la Commissione europea dovesse concludere che la Svizzera, o singoli Cantoni, non dovessero più garantire l'adeguatezza del diritto della protezione dei dati.

Per l'ampiezza e la portata delle modifiche, che tengono conto anche dell'evoluzione del diritto e delle prassi cantonali, la legge cantonale sulla protezione dei dati viene rivista integralmente (revisione totale).

II. CONTESTO LEGISLATIVO

1. Consiglio d'Europa

Convenzione STE 108

Il Consiglio d'Europa ha portato a termine nel 2016 un processo di modernizzazione della Convenzione STE 108 del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e del suo Protocollo aggiuntivo STE 181 dell'8 novembre 2001 concernente le autorità di controllo e i flussi internazionali di dati. La revisione è tesa a consentire di affrontare meglio le sfide che la globalizzazione, l'evoluzione tecnologica e l'aumento del flusso internazionale di dati presentano, attraverso la garanzia dell'autonomia personale fondata sul diritto della persona di controllare i propri dati personali e l'elaborazione di cui sono oggetto. Il Protocollo di emendamento della STE 108 prevede, tra l'altro, il rafforzamento dei diritti delle persone interessate e dei corollari obblighi del titolare di un trattamento di dati, l'obbligo di istituire un'autorità di controllo indipendente e imparziale, con le risorse necessarie per adempiere in modo effettivo ed efficace le proprie funzioni e per esercitare i suoi poteri, consistenti essenzialmente nell'apertura d'inchieste, nell'infliggere sanzioni amministrative e nella facoltà di stare in giustizia. L'autorità di controllo deve essere autorizzata a prendere decisioni vincolanti impugnabili e a pronunciare sanzioni amministrative. D'altra parte, la STE 108 agevola la comunicazione di dati tra gli Stati parte e l'accesso delle imprese svizzere ai mercati degli altri Stati parte. I lavori di revisione della STE 108 e del suo Protocollo aggiuntivo si sono conclusi nel giugno del 2016.

Il 19 giugno 2020, il Parlamento svizzero ha approvato la ratifica del Consiglio federale del 30 ottobre 2019 del Protocollo di emendamento alla Convenzione STE 108. La ratifica è vincolante anche per i Cantoni, che sono obbligati ad adempiere i nuovi requisiti previsti dal Protocollo di emendamento e a recepirli nel loro diritto. La Svizzera ha ratificato il Protocollo d'emendamento della STE 108, sia per ragioni inerenti alla tutela dei diritti dell'uomo, sia per ragioni economiche (agevolazione della comunicazione transfrontaliera di dati), sia per non compromettere la decisione di adeguatezza del diritto svizzero della protezione dei dati.

2. Unione europea

L'Unione europea ha, dal canto suo, emanato due nuovi atti normativi, uno generale sulla protezione dei dati (Regolamento (UE) 2016/679), l'altro specifico al settore della polizia e del giudiziario penale (Direttiva (UE) 2016/680). Ambedue i nuovi atti normativi UE hanno iniziato a espletare pienamente i loro effetti giuridici a partire dal 25 maggio 2018, dopo un periodo transitorio di adeguamento di due anni. Perseguono essenzialmente gli scopi di garantire *a)* la protezione dei diritti e delle libertà fondamentali nella società digitale, *b)* la lotta al terrorismo e alla criminalità, assicurando la libera circolazione delle rispettive informazioni tra le autorità competenti, nel rispetto dei diritti e delle libertà fondamentali delle persone interessate e *c)* l'ottimizzazione dell'economia tramite la libera circolazione dei dati e l'aumento della competitività del mercato grazie a nuove attività economiche legate alla società digitale.

a. Regolamento (UE) 2016/679 (GDPR)

L'Unione europea ha riveduto la propria legislazione sulla protezione dei dati, sostituendo innanzitutto la Direttiva 95/46 CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, con il nuovo Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (noto anche come GDPR – General Data Protection Regulation).

A partire dal 25 maggio 2018, le elaborazioni di dati che soggiacciono al campo di applicazione del Regolamento (UE) 2016/679 devono avvenire a determinate condizioni, altrimenti possono cadere, tra l'altro, sotto il suo regime sanzionatorio. Rientrano, innanzitutto, nel campo di applicazione del Regolamento (UE) 2016/679 tutte le elaborazioni di dati personali da parte di organizzazioni (anche svizzere) che hanno una sede sul territorio dell'Unione europea e che concernono persone che si trovano nell'Unione. Oltre a ciò, in virtù del principio di extra-territorialità (o del luogo di mercato, art. 3 Regolamento (UE) 2016/679), il Regolamento espleta i suoi effetti anche su elaborazioni di dati personali da parte di entità private o pubbliche svizzere con sede in Svizzera, nella misura in cui concernono persone che si trovano nell'Unione. Secondo tale principio, le aziende site al di fuori dell'Unione europea che offrono o promuovono attivamente (principalmente, tramite internet) i loro beni o servizi a cittadini che si trovano nell'Unione, soggiacciono alle stesse regole valide per le aziende con sede nell'Unione. Rientra nel campo di applicazione del Regolamento (UE) 2016/679 secondo lo stesso principio anche la promozione mirata a persone che si trovano nell'Unione europea tramite tecniche di profilazione individuale del comportamento, di abitudini o di preferenze (ad esempio, cookies). Il principio del luogo di mercato è inteso creare condizioni di concorrenza uguali in materia di protezione dei dati per tutte le aziende attive sul mercato europeo.

A differenza della Direttiva (UE) 2016/680 e della STE 108, la Svizzera non è vincolata al Regolamento (UE) 2016/679, poiché non costituisce parte integrante dell'*acquis* di Schengen, né rappresenta un trattato internazionale in altro modo vincolante per la Svizzera. Non è quindi tenuta a recepirlo e attuarlo. La Svizzera intende tuttavia allinearvi, in parte, il proprio diritto, per non compromettere la decisione dell'Unione europea di adeguatezza del diritto svizzero della protezione dei dati e, quindi, in particolare, gli

interessi economici del nostro Paese e la rispettiva, libera circolazione dei dati. La decisione di adeguatezza dell'Unione europea garantisce, infatti, all'economia di Paesi terzi come la Svizzera il libero scambio di merci e servizi e dei relativi dati personali con l'Unione, senza ulteriori condizioni (convenzioni sulla protezione dei dati).
L'entrata in vigore del Regolamento (UE) 2016/679 tocca essenzialmente l'economia privata e solo eccezionalmente lo Stato, poiché quest'ultimo non è, di regola, attivo sul territorio dell'Unione europea ai sensi dell'articolo 3 Regolamento (UE) 2016/679. Tenuto conto in particolare del regime sanzionatorio previsto dal Regolamento, l'Incaricato cantonale della protezione dei dati ha comunque chiamato il Cantone, gli enti locali e chi assume compiti di Stato in Ticino a valutare se rientrano, eccezionalmente, nel suo campo di applicazione nei loro vari settori di attività (ad esempio, in caso di campagne pubblicitarie o di profilazioni mirate verso cittadini dell'Unione da parte di aziende o enti statali o parastatali) e ad adottare, se del caso, le necessarie misure per adeguarsi.

b. Direttiva (UE) 2016/680

L'Unione ha abrogato la Decisione quadro 2008/977/GAI del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale e ha promulgato in sua vece la Direttiva (UE) 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. La Direttiva (UE) 2016/680 è parte dell'*acquis* di Schengen, vale a dire dell'insieme di disposizioni volte alla realizzazione della libera circolazione delle persone senza controlli alle frontiere e che prevede misure compensative che consentono di garantire un alto livello di sicurezza. Tale insieme di norme consiste nell'Accordo di Schengen del 1985, nella Convenzione di applicazione e completamento del 1990, nei successivi trattati di adesione e nelle ulteriori normative applicabili in virtù degli accordi di Schengen come, appunto, la Direttiva 680 in materia di protezione dei dati.

Alla stessa stregua della Convenzione STE 108 del Consiglio d'Europa, la Direttiva (UE) 2016/680 prevede in particolare il rafforzamento di diritti e degli obblighi delle persone interessate, rispettivamente dei titolari del trattamento di dati, nonché delle condizioni per la trasmissione internazionale di dati. In particolare, prevede l'obbligo dei titolari di elaborazioni di dati di tenere il registro delle banche dati. Istituisce l'obbligo della valutazione d'impatto, da sottoporre all'autorità di vigilanza in materia di protezione dei dati, qualora un'elaborazione di dati presenti un rischio elevato per i diritti e le libertà delle persone. Prevede l'obbligo di istituire un'autorità di vigilanza pienamente indipendente, al fine di garantire una effettiva tutela dei diritti e delle libertà fondamentali in relazione all'elaborazione di dati personali. Secondo la Direttiva, l'autorità di vigilanza non deve subire pressioni di nessun tipo, né dirette, né indirette, e non può sollecitare o accettare istruzioni da nessuno. L'autorità di vigilanza deve inoltre essere dotata di risorse umane, tecniche e finanziarie adeguate, per l'effettivo e credibile adempimento dei propri compiti e per l'esercizio dei propri poteri.

L'UE ha notificato alla Svizzera la Direttiva (UE) 2016/680 in quanto *acquis* di Schengen, che la Svizzera quale Paese associato allo spazio Schengen è tenuta a recepire se non vuole compromettere gli accordi di Schengen, in particolare l'accesso delle autorità svizzere di polizia al sistema d'informazione di Schengen SIS. La Svizzera ha notificato

l'accettazione della Direttiva il 1° settembre 2016. Le rispettive norme federali di attuazione della Direttiva sono entrate in vigore il 1° marzo 2019. (vedi legge federale del 28 settembre 2018 che attua la direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali [Sviluppo dell'*acquis* di Schengen]; FF 2018 5079).

III. PRINCIPALI NOVITÀ LEGISLATIVE

Il nuovo diritto internazionale è fondato sul rafforzamento di principi quali la limitazione della raccolta e dell'elaborazione dei dati (o principio della parsimonia dei dati), la trasparenza dell'elaborazione, la protezione dei dati in funzione dei rischi, la qualità dei dati e la sicurezza. Prevede inoltre il consolidamento dei diritti delle persone e delle responsabilità dei titolari delle elaborazioni, in particolare gli obblighi della valutazione d'impatto di un'elaborazione sui diritti della persona nel caso in cui l'elaborazione possa presentare un rischio elevato per gli stessi, della protezione dei dati sin dalla progettazione di un'elaborazione (privacy by design) e per impostazione predefinita (privacy by default), della consultazione preventiva dell'Incaricato per elaborazioni che presentano rischi qualificati per la persona e l'obbligo della notifica della violazione della protezione dei dati all'autorità di vigilanza sulla protezione dei dati. Ulteriori elementi fondamentali della revisione sono il potenziamento del controllo da parte degli incaricati della protezione dei dati, della protezione dei minori (necessità del consenso dell'autorità parentale per l'uso di servizi della società dell'informazione) e del regime sanzionatorio. D'altro canto, è previsto il miglioramento della trasmissione transfrontaliera di dati. Con tali principi, s'intende creare il giusto equilibrio tra il libero flusso di informazioni e la protezione della persona.

Peculiarmente ai diritti delle persone, sono previste le seguenti modifiche:
- principio della trasparenza: il titolare dell'elaborazione è tenuto a fornire all'interessato informazioni di dettaglio relative all'elaborazione di dati che lo concernono; l'informativa deve essere facilmente accessibile e di facile comprensione, in particolar modo nel caso di informazioni a minori;
- diritto di accesso: sono ampliate le categorie d'informazioni riguardanti l'elaborazione di dati da fornire all'interessato in caso di richiesta di accesso ai propri dati;
- diritti di rettifica e di cancellazione: sono da garantire senza ingiustificato ritardo;
- diritto all'oblio: nel caso in cui dati personali sono stati trasmessi a terzi, il titolare dovrà informarli della richiesta di rettifica, cancellazione o distruzione dei dati effettuata da parte della persona interessata;
- diritto alla limitazione del trattamento: in alcuni casi previsti dalla legge, l'interessato può ottenere la limitazione del trattamento dei suoi dati personali; il titolare potrà soltanto conservare i dati, senza possibilità di ulteriori operazioni su di essi;
- diritto alla portabilità dei dati: su richiesta, il titolare del trattamento deve mettere a disposizione dell'interessato i suoi dati personali su adeguato supporto portatile;
- diritto di opposizione: l'interessato può opporsi a qualsiasi trattamento che lo riguarda, riservata l'esistenza di un interesse preponderante o di una legge;
- diritto a non essere sottoposto a processo decisionale esclusivamente automatizzato;
- diritto alla comunicazione di una violazione dei dati personali: il titolare del trattamento è tenuto a comunicare all'interessato le violazioni dei dati personali suscettibili di presentare un elevato rischio per i suoi diritti e le sue libertà.

Per quanto riguarda gli obblighi dei titolari di elaborazioni di dati, è previsto in particolare:
- principio della responsabilità: il titolare dell'elaborazione è attivamente responsabile di agire in conformità con il diritto sulla protezione dei dati e, in particolare, di comprovare che l'elaborazione avviene in conformità con quest'ultimo (inversione dell'onere della prova a carico del titolare dell'elaborazione di dati);
- principio dell'approccio basato sui rischi: maggiore è il rischio per i diritti e le libertà fondamentali, maggiori sono le responsabilità del titolare del trattamento, che dovrà in particolare mettere in atto misure di sicurezza adeguate ai rischi e meccanismi e sistemi di controllo del rispetto del diritto;
- principio della protezione dei dati fin dalla progettazione (Privacy by design) e per impostazione predefinita (privacy by default): le garanzie della protezione dei dati devono essere prese in considerazione sin dalla progettazione dei prodotti e dei servizi;
- obbligo del registro delle elaborazioni di dati: ogni grande impresa privata o organo pubblico che elabora dati personali deve tenere un registro delle proprie attività di elaborazione;
- obbligo della valutazione d'impatto sulla protezione dei dati nei casi in cui un'elaborazione possa presentare un rischio elevato per i diritti e le libertà fondamentali degli interessati; se sono evidenziati rischi particolari, il titolare del trattamento dovrà consultare l'autorità di controllo indipendente;
- obbligo di auto-segnalazione: Il titolare deve notificare all'autorità di controllo indipendente e, in taluni casi, anche alla persona interessata, le violazioni dei dati personali da lui perpetrate, senza ingiustificato ritardo, affinché l'autorità di controllo possa esercitare le sue mansioni legali;
- obbligo della sicurezza delle elaborazioni: questo principio implica l'implementazione di misure commisurate ai rischi per i diritti e le libertà fondamentali;
- obbligo di un'autorità di controllo pienamente autonoma e indipendente: l'autorità di controllo deve agire in piena autonomia e indipendenza e disporre di tutte le risorse umane, tecniche e finanziarie necessarie per l'effettivo adempimento dei suoi compiti legali.

IV. COMMENTO SUI SINGOLI ARTICOLI

Articolo 1
Il campo di applicazione della LPDP (art. 1 LPDP) non si limita ai soggetti previsti dall'attuale articolo 2, ma si estende anche alle procedure speciali e alle relative autorità (nuovo art. 4 LPDP). Con la presente revisione si propone di sostituire il richiamo all'attuale articolo 2 LPDP con quello relativo ai nuovi articoli 3 e 4 LPDP concernenti il campo di applicazione.

Articoli 2-4 Campo di applicazione
Gli attuali articoli 2 e 3 concernenti il campo di applicazione della LPDP vengono riformulati in tre disposizioni, per garantirne maggiore chiarezza e per meglio integrarvi le necessarie modifiche imposte dal diritto superiore. Il campo di applicazione viene suddiviso in campo d'applicazione materiale (art. 2), istituzionale e personale (art. 3) e procedurale (art. 4).

Articolo 2
Il nuovo articolo 2 LPDP corrisponde all'attuale articolo 2 capoverso 1 LPDP. A parte il nuovo titolo marginale, la norma viene rettificata quanto ai concetti "modi e procedure

utilizzati" i quali, allineandosi al nuovo diritto superiore, vengono sostituiti con "procedure e modalità utilizzate".

Articolo 3
L'attuale articolo 2 capoverso 2 sui soggetti alla LPDP concerne tra l'altro le persone fisiche e giuridiche di diritto privato quali mandatari di compiti pubblici. Per distinguere il mandato di compiti pubblici dal mandato di elaborazioni di dati (nuovo art. 23 del presente disegno di legge), il nuovo articolo 3 capoverso 1 riprende il concetto di delega di compiti di diritto pubblico. Copre sia le deleghe di compiti legali previste dalla legge, sia altre deleghe su base convenzionale, statutaria, con mandato di prestazione, ecc. Per il resto, l'attuale articolo 2 capoverso 2 LPDP non subisce variazioni.

Rientrano nel concetto di corporazioni o istituti di diritto pubblico secondo il nuovo articolo 3 capoverso 1, secondo periodo, tra l'altro, i seguenti organismi statali e parastatali: i consorzi di comuni in base alla legge sul consorziamento di comuni del 20 febbraio 2010, i consorzi in base alla legge sui consorzi del 1913, i consorzi per il raggruppamento terreni in base alla legge sul raggruppamento e la permuta dei terreni del 23 novembre 1970, i patriziati, le parrocchie, l'Istituto delle assicurazioni sociali (IAS) e organi subordinati quali la Cassa cantonale di compensazione, l'Università della Svizzera italiana (USI), la Scuola Universitaria professionale della Svizzera italiana (SUPSI), l'Ente ospedaliero cantonale (EOC), l'Azienda elettrica ticinese (AET), l'Azienda cantonale dei rifiuti (ACR), gli istituti autonomi comunali quali i Trasporti pubblici del Luganese (TPL), le Aziende industriali del Luganese (AIL), gli ordini cantonali (dei medici, farmacisti, avvocati, notai, veterinari, ecc.).

Sono invece delegatari di compiti di diritto pubblico attraverso delega legislativa, concessione, mandato di prestazione, contratto, ecc., ad esempio i servizi di assistenza e cura a domicilio (SACD) secondo la Legge sull'assistenza e cura a domicilio del 30 novembre 2010, altri organismi cui sono assegnati compiti pubblici in ambito sanitario secondo la Legge concernente il promovimento, il coordinamento e il finanziamento delle attività a favore delle persone anziane del 30 novembre 2010, i servizi cui sono affidati compiti pubblici secondo la legge sull'integrazione sociale e professionale degli invalidi del 14 marzo 1979, i servizi pre-ospedalieri e di soccorso secondo la rispettiva Legge del 26 giugno 2001, gli organismi che curano programmi occupazionali, le istituzioni o società beneficiarie di un mandato di prestazione quali le cliniche private, le case per anziani, la Società epilettici della Svizzera italiana, aziende delegatarie di trasporti pubblici in base alla legge sui trasporti pubblici del 6 dicembre 1994, le società anonime, le cooperative o le associazioni cui i comuni assegnano compiti e servizi pubblici (ad esempio, per l'approvvigionamento di acqua potabile), ecc. I delegatari di compiti pubblici sono sottoposti alla LPDP nella misura in cui la loro attività specifica rientra nell'ambito della delega. Per il resto, sono considerati dei privati e le loro elaborazioni soggiacciono alla legge federale sulla protezione dei dati.

Quando un organismo secondo il capoverso 1 non agisce nell'ambito del compito pubblico affidatogli, quindi quando non agisce come autorità che per legge detiene un potere pubblico, ma è soggetto alla concorrenza economica, le rispettive elaborazioni di dati sono sottoposte alle disposizioni della legge federale sulla protezione dei dati applicabili ai privati (capoverso 2). In virtù di una convenzione tra Incaricato federale della protezione dei dati e della trasparenza e Incaricati cantonali, la sorveglianza della corretta applicazione di tali norme federali compete all'Incaricato cantonale della protezione dei

dati, che agisce secondo le norme cantonali sulla sorveglianza (vedi art. 37 lett. b del presente disegno di legge).

Articolo 4
Il primo capoverso riprende e riformula l'attuale articolo 3 capoverso 1 terza frase LPDP, secondo il quale la legge è sempre applicabile alla procedura di prima istanza. Si è ritenuto opportuno riposizionare questo disposto, prevedendo innanzitutto le procedure nelle quali la LPDP è sempre applicabile e lasciando al secondo, nuovo capoverso, il disciplinamento delle restrizioni al campo di applicazione procedurale.

Alle procedure amministrative di prima istanza, ossia quelle procedure che sfociano in una decisione di un'autorità amministrativa, si applica, come finora, la LPDP, in concorrenza con la LPAmm. Nelle procedure di prima istanza rientrano anche le procedure di reclamo (ne è esempio, in diritto fiscale, la procedura su reclamo che porta a una [seconda] decisione soggetta a ricorso alla Camera di diritto tributario del Tribunale d'appello, oppure, in diritto delle assicurazioni sociali, la procedura su opposizione che porta l'assicurazione a emettere una [seconda] decisione ex articolo 52 LPGA impugnabile con ricorso al Tribunale cantonale delle assicurazioni).

Ritenuta la concorrenza tra le due normative, in ambito di prima istanza può sorgere un possibile conflitto normativo tra di esse, che in pratica si riduce alla questione dell'accesso agli atti. A quest'ultimo può applicarsi sia il diritto di accesso secondo la LPDP, sia il diritto di essere sentito (ante procedura) secondo gli articoli 32 e seguenti LPAmm, che discende dal diritto di essere sentito (e il corollario diritto di consultare gli atti) di cui all'articolo 29 capoverso 2 Cost./CH. L'interessato valuta su quale diritto fondare la sua richiesta di accesso in funzione dello scopo che persegue e delle rispettive necessità informative nel caso concreto, tenendo conto delle considerazioni seguenti: Il diritto di consultare gli atti sgorgante dall'articolo 29 capoverso 2 Cost./CH è in stretta correlazione con il diritto di accesso della protezione dei dati dedotto, a livello costituzionale, dagli articoli 10 capoverso 2 e 13 capoverso 2 Cost./CH. Fondate su basi costituzionali diverse, le due garanzie non sono però equivalenti: ciascuna ha il suo campo d'applicazione ed esse possono essere invocate indipendentemente l'una dall'altra. La portata del diritto d'accesso è più ristretta poiché non si estende a tutti gli atti determinanti per l'esito della procedura, ma unicamente alle informazioni concernenti la persona interessata; essa è però anche più ampia, poiché il diritto di accesso può essere esercitato indipendentemente da una procedura specifica, senza che l'interessato debba potersi prevalere, riservato l'abuso di diritto, di un interesse legittimo concreto. Inoltre, alcune distinzioni proprie del diritto di esaminare gli atti sono prive di pertinenza nell'ambito della protezione dei dati. Ciò vale in special modo per la distinzione – non sempre agevole e criticata in dottrina – fra gli atti che le parti possono esaminare e i cosiddetti atti interni dell'amministrazione: il diritto di accesso della protezione dei dati, infatti, contempla anche i documenti interni (tanto più se contengono dati sensibili), che sono invece costantemente sottratti a consultazione nella procedura amministrativa, non essendo una simile facoltà inclusa nel diritto di esaminare gli atti. Rimangono riservati i casi in cui la decisione amministrativa menziona gli atti interni. Il diritto di consultare gli atti garantito dall'articolo 29 capoverso 2 Cost./CH non è assoluto e può essere limitato a tutela di interessi pubblici o privati preponderanti (Messaggio n. 6645 del 23 maggio 2018 relativo alla revisione totale della legge di procedura per le cause amministrative del 19 aprile 1966, pag. 19).

L'attuale articolo 3 capoverso 1 LPDP disciplina il rapporto tra LPDP e il diritto procedurale e stabilisce come principio generale che le elaborazioni di dati nell'ambito di tutti i procedimenti pendenti sono rette dal rispettivo codice di procedura. Più esattamente, la norma sancisce che quando una procedura civile, penale o amministrativa è in corso (ad eccezione di quella di prima istanza, vedi cpv. 1), la protezione dei dati è garantita dalle legislazioni speciali. Allineandosi al disegno di nuova legge federale sulla protezione dei dati, questa norma viene precisata nel capoverso 2, prevedendo che il trattamento di dati personali e i diritti delle persone interessate nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali sono retti dal diritto procedurale applicabile. Rispetto al diritto vigente non si parla quindi più unicamente di procedimenti pendenti, ma di procedimenti giudiziari o disciplinati da un ordinamento procedurale federale o cantonale, che non configurano necessariamente ancora un procedimento pendente stricto sensu (vedi ad esempio art. 74 cpv. 2 CPP). Per procedimenti giudiziari s'intendono tutti i procedimenti contenziosi dinanzi a tribunali penali, civili e amministrativi cantonali o federali nonché i tribunali arbitrali con sede in Svizzera. I procedimenti giudiziari sono quelli che si svolgono dinanzi a un giudice che si occupa per la prima volta di un caso per il quale il procedimento è stato avviato conformemente all'ordinamento procedurale determinante. Un procedimento è disciplinato dagli ordinamenti procedurali federali (in particolare PA, CPP, CPC, LTF, LTAF, LTFB, LEF, DPA, PPM, AIMP) o cantonali (LPAmm), non appena un'autorità tratta una determinata fattispecie conformemente alle disposizioni di una delle suddette leggi. Può rientrare nel concetto di procedimento giudiziario anche la procedura di petizione davanti al Tram quale istanza unica (art. 92 LPAmm), ritenuto che in tale procedura non si è confrontati a un provvedimento amministrativo emanato autoritariamente e suscettibile di ricorso, bensì ad una pretesa fatta valere davanti a un tribunale nella quale l'ente pubblico figura come parte (cfr. Borghi/Corti, Compendio di procedura amministrativa ticinese, commento ad art. 71 LPAmm). Le modalità di presentazione della petizione e della risposta sono quelle della procedura civile a cui rinviavano gli articoli 72 e 73 capoverso 1 della previgente legge di procedura per le cause amministrative del 19 aprile 1966, oggi codificati agli articoli 93 e 94 LPAmm (cfr. Messaggio n. 6645 del 23 maggio 2012 inerente la revisione totale della legge di procedura per le cause amministrative del 19 aprile 1966, pag. 61 e seguenti).
Non rientrano per contro nel campo di applicazione del nuovo articolo 4 capoverso 2 le procedure di vigilanza, quale quella prevista dalla Legge organica comunale.
Riassumendo, il criterio determinante per l'applicabilità o meno della LPDP, è l'assenza o la presenza, sotto il profilo funzionale, di un rapporto diretto con un ordinamento procedurale. Un tale rapporto sussiste in particolare se il trattamento di dati personali in questione può avere ripercussioni concrete sul procedimento o sul suo esito oppure sui diritti procedurali delle parti.

Laddove, in un procedimento giudiziario o disciplinato da un ordinamento procedurale, il diritto procedurale federale o cantonale non è equivalente alla LPDP in materia di protezione dei dati, si applica la LPDP. In tal caso, tuttavia, l'organo decisionale non soggiace alla sorveglianza dell'Incaricato cantonale della protezione dei dati. La LPDP si applica nella misura in cui non collide con norme specifiche dell'ordinamento procedurale applicabile. L'intimazione di un ricorso alla controparte, e il loro diritto di essere sentiti, non può, ad esempio, essere bloccato, rispettivamente precluso da parte del ricorrente, sulla base del diritto di blocco previsto dalla LPDP. In questo senso, la LPDP va intesa come legge generale e sussidiaria tesa a completare l'ordinamento procedurale laddove

quest'ultimo dovesse essere lacunoso o non dovesse garantire la protezione dei dati in modo equivalente alla LPDP.

Dopo la conclusione del procedimento in materia penale, l'elaborazione dei dati personali, la procedura e la tutela giurisdizionale sono retti dalle disposizioni della Confederazione e dei Cantoni in materia di protezione dei dati (art. 99 cpv. 1 CPP).

In materia civile, quando la causa entra in forza di cosa giudicata formale, la procedura è terminata e si riapplica la legge federale sulla protezione dei dati (LPD).

In materia amministrativa cantonale, una volta la causa entrata in forza di cosa giudicata formalmente, si applica la presente legge sulla protezione dei dati. Negli altri casi, va valutato quale normativa sulla protezione dati sia applicabile a procedimento concluso.

Articolo 5
Contrariamente al legislatore federale, a livello cantonale si è scelto di mantenere la protezione delle persone giuridiche e ciò per svariati motivi (capoverso 1). In *primis* perché la rinuncia alla protezione delle persone giuridiche nel disegno di legge federale (D-LPD) non implica che le persone giuridiche non abbiano più una personalità o che esse siano, ora, privi di meccanismi di difesa. Di fatto, resta immutata l'ampia protezione garantita dagli articoli 28 e seguenti (lesioni della personalità, ad esempio della reputazione) del Codice civile svizzero, dalla LCSI, dalla legge federale sul diritto d'autore del 9 ottobre 1992 o dalle regole sul segreto professionale, d'affari o di fabbricazione, nonché dall'articolo 13 Cost./CH Inoltre, l'articolo 5 Cost./CH esige che l'attività dello Stato sia retta dalla legge e ciò implica la necessità di creare delle basi legali per l'elaborazione di dati personali da parte di organi pubblici. Richiamato l'articolo 5 Cost./CH, il legislatore federale ha dovuto introdurre nella LOGA una serie di disposizioni che disciplinano il trattamento di dati di persone giuridiche da parte di organi federali, le quali sostituiscono, de facto, le norme contenute nella LPD. Riprendere lo stesso meccanismo a livello cantonale avrebbe implicato la necessità di inserire delle norme ad hoc che autorizzassero gli organi cantonali a trattare i dati personali delle persone giuridiche nelle varie basi legali settoriali del diritto cantonale. Ciò comporterebbe un'inflazione normativa, oltre a creare una certa insicurezza giuridica.

In analogia al diritto federale, il capoverso 2 contempla, ora, delle categorie definite di dati che meritano una protezione particolare, dovuta all'impatto particolarmente importante che la loro elaborazione può avere, per la loro natura o la loro funzione, sulla personalità della persona interessata. Con il nuovo diritto l'elenco di dati meritevoli di particolare protezione, sinora esemplificativo, diventa quindi esaustivo. La definizione di dato sensibile è esclusiva: sono considerati tali soltanto i dati specificamente indicati nella legge, indipendentemente dal carattere di riservatezza o di particolare rilevanza che un individuo, o il senso comune, può attribuire ad altre tipologie di dati. In caso di elaborazioni di dati sensibili i principi generali della protezione dei dati vanno applicati con più rigore, ad esempio quando il consenso è necessario per l'elaborazione dei dati, quest'ultimo deve essere esplicito se si tratta di dati sensibili; oppure in caso di elaborazioni sistematiche di dati sensibili il motivo giustificativo deve necessariamente essere una base legale formale.

a. Queste *opinioni o attività* appartengono alle credenze e convinzioni intime della persona. Le opinioni filosofiche vanno intese in senso lato, come concezione della vita,

del mondo; modo in cui singoli individui o gruppi sociali considerano l'esistenza e i fini del mondo e la posizione dell'uomo in esso e non solamente come il fatto di seguire una dottrina filosofica specifica. Questi dati sono protetti in modo particolare indipendentemente della loro portata; l'informazione concernente l'appartenenza anche solamente passiva ad un'organizzazione, un partito o una comunità religiosa è un dato sensibile.

b. In conformità con la direttiva (UE) 2016/680 e il regolamento (UE) 2016/679, la nozione di dati personali degni di particolare protezione è estesa ai dati relativi all'*appartenenza etnica*. Sebbene i termini razza e etnia siano utilizzati in parallelo, il concetto di appartenenza ad una razza deve essere inteso nel senso più ampio e contemporaneo di appartenenza ad un'etnia. Questa categoria è problematica in caso di elaborazioni tramite apparecchi di videosorveglianza. Infatti, anche una ripresa d'immagini perfettamente innocua, può rivelare per definizione la razza (bianca o nera o altro) di una persona. Bisogna in questo caso, nell'ottica dell'adeguatezza sociale, tenere conto del contesto e dello scopo principale dell'elaborazione di ripresa di immagini (foto o video). Lo scopo principale di queste norme è evitare la determinazione dei profili in base all'etnia o alla razza (*profiling* etnico), ossia l'uso da parte delle autorità di generalizzazioni derivanti da etnia, razza, religione o origine nazionale – e non in base a elementi obiettivi o comportamenti individuali – come base per le decisioni delle autorità (ad esempio in ambito di polizia). Con tale scelta legislativa si è voluto assicurare la tutela dell'individualità, in condizioni di parità, delle libertà fondamentali dell'uomo in ogni settore della vita pubblica, in particolare nel campo politico, sociale, economico e culturale.

c. Si tratta di tutte le informazioni che permettono, direttamente o indirettamente, di trarre delle conclusioni sullo *stato di salute, fisico, mentale o psichic*o di una persona. Ad esempio la diagnosi medica, così come la semplice ricetta o la fattura per un medicamento sono dati relativi alla salute e quindi sensibili. La nozione ha un carattere molto lato e elastico che può portare a dei risultati paradossali. Onde evitare situazioni che possano essere assurde, occorre analizzare ogni situazione nell'ottica degli usi sociali abituali, tenendo conto del contesto dell'elaborazione del dato, dell'importanza materiale delle informazioni rivelate sulla persona o dell'impatto che la rivelazione del dato può avere su di essa. Così, la ricetta di lenti a contatto non presenta lo stesso grado di sensibilità d'una diagnosi medica e non soggiace alle stesse condizioni di tutela.

d. Sono considerati dati sulla *sfera intima* in particolare i dati sulla vita e l'orientamento sessuali della persona interessata (cfr. anche P-STE 108 [art. 6 par. 1], direttiva [UE] 2016/680 [art. 10] e regolamento [UE] 2016/679 [art. 9]). Anche l'identità sessuale di una persona rientra nella sfera intima.

e. I *dati genetici* sono informazioni sul patrimonio genetico di una persona ottenute attraverso un esame genetico; ne fa parte anche il profilo del DNA (art. 3 lett. l della legge federale sugli esami genetici sull'essere umano dell'8 ottobre 2004). Per essere considerati dati sensibili, questi dati devono necessariamente basarsi su un processo tecnico che permetta l'identificazione e l'autenticazione univoca della persona.

f. In generale, i *dati biometrici* sono quei dati personali che si ricavano da caratteristiche fisiche o comportamentali uniche e identificative di ciascuna persona fisica. Fanno parte di questa categoria di dati, ad esempio, le impronte digitali, la specifica conformazione fisica della mano o del volto, dell'iride o della retina, la firma grafometrica (ovvero quella firma elettronica effettuata su apposito supporto mediante un gesto fisico in tutto coincidente con quello utilizzato per firmare su carta), nonché il

timbro e la tonalità della voce, a partire dal momento che permettono di identificare una persona in modo univoco. I dati biometrici sono dati personali nella misura in cui possono essere associati a una persona identificata o identificabile. Dal punto di vista normativo, l'articolo 4 paragrafo 1 n. 14 del Regolamento (UE) 2016/679, definisce i dati biometrici come quei "dati personali ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica e che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici". Nel caso di normali fotografie, ad esempio, questa premessa non è data.

g. Questa norma è applicabile, oltre che ai dati relativi a *procedure civili e amministrative*, anche a quelli risultanti da perseguimenti e sanzioni della *giurisdizione penale ordinaria e militare*. Entrano in considerazione anche le sanzioni disciplinari emesse non solo da organi pubblici ma anche da associazioni private che hanno un monopolio di fatto in un determinato settore d'attività della persona interessata (ad esempio una sanzione per doping pronunciata da un'associazione sportiva). La protezione è data anche quando questi perseguimenti o sanzioni sono stati emessi da autorità estere.
h. Si tratta dell'*aiuto sociale individuale* fornito dalla collettività alle persone che sono in situazioni sociali e/o economiche di bisogno (presa a carico sociale e/o economica) ai sensi del diritto federale e cantonale sull'assistenza sociale. Le misure relative all'assicurazione sociale non rientrano nelle misure di assistenza sociale ai sensi della presente legge. Parimenti, le misure tutelari stabilite dal Codice civile svizzero non sono considerate misure di assistenza sociale ai sensi della presente legge, esse sono tutelate dalle norme speciali sul segreto tutorio.

Con il termine elaborazione di dati personali s'intende qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati. Con distruzione dei dati s'intende quella fisica definitiva (capoverso 3)

L'elaborazione puntuale si limita esplicitamente al singolo caso, vale a dire quando avviene un'unica volta, per uno scopo unico e non ripetibile (singolarità dell'evento), indipendentemente dal fatto che implichi l'elaborazione dei dati di una o più persone. Ciò significa che l'elaborazione puntuale si svolge entro determinati e limitati margini temporali. Tipicamente, si tratta di trasmissioni di dati, ad esempio, la trasmissione di dati del controllo abitanti riguardanti una o più persone solidalmente responsabili, su richiesta scritta e motivata di un terzo, per la riscossione di suoi crediti (capoverso 4).

Per opposizione all'elaborazione puntuale, l'elaborazione sistematica implica una pluralità, o ripetizione, di elaborazioni di dati in una successione temporale (capoverso 5). Può trattarsi di una successione di elaborazioni diverse tra di loro concernenti gli stessi dati (ad esempio, raccolta di dati anagrafici di una persona, loro registrazione in una banca dati, utilizzazione ripetuta per l'esecuzione di compiti legali, modifica, trasmissione a terzi su richiesta, archiviazione e distruzione), oppure di un determinato tipo di elaborazione ripetuto nel tempo (ad esempio, l'accesso, regolare o irregolare, ai dati personali di una determinata persona tramite procedura di richiamo), oppure ancora di una loro

combinazione (raccolta, registrazione, trasmissione dei dati a uno o più terzi tramite procedura di richiamo, su arco di tempo prolungato o indeterminato).

È considerato interfacciamento o associazione di banche dati il collegamento per sincronizzare i dati tra il fornitore di dati e l'utente dei dati, senza che quest'ultimo debba farne esplicita richiesta presso il fornitore dei dati o debba accedervi tramite procedura di richiamo (capoverso 7).

Contrariamente alla norma federale, a livello cantonale la nozione di banca dati (o collezione, rispettivamente archivio di dati) non è stata abrogata, bensì ridefinita, ampliandone il campo di applicazione (capoverso 8). Il concetto di banca dati comprende ora non soltanto gli insiemi di dati strutturati (esistenza di un nesso logico tra le informazioni ivi contenute), ma anche quelli non strutturati, quali ad esempio i server contenenti videoregistrazioni. Questi ultimi vanno infatti considerati, a tutti gli effetti, come delle vere e proprie banche dati. La definizione di banca dati prescinde quindi, ora, dalla strutturazione o meno degli insiemi di dati elaborati. Inoltre, nella nuova definizione di banca dati rientrano non più soltanto gli insiemi di dati gestiti in modo centralizzato e in un unico supporto, ma pure quelli gestiti in modo decentralizzato, oppure ripartiti in più supporti o ubicazioni. Per il resto le caratteristiche della banca dati sono rimaste immutate, indipendentemente dal supporto fisico di memorizzazione o dalla funzione che devono assolvere, i dati devono essere rappresentati in un formato che renda possibile la loro interpretazione; devono essere registrati su un supporto che ne renda possibile la scrittura e la rilettura anche a distanza di tempo; devono essere organizzati in modo da permettere una facile consultazione.

Nel capoverso 9 il termine proposto di profilazione designa il processo automatizzato di valutazione di determinate caratteristiche di una persona stilata sulla base di dati personali ottenuti tramite elaborazione automatica e finalizzati soprattutto all'analisi e alla previsione di interessi, performance lavorative, condizioni economiche e di salute, comportamento, luogo di dimora e mobilità, ecc., al fine di prendere misure e decisioni commisurate al soggetto. La profilazione si ha quindi in presenza di 3 elementi: 1. un trattamento automatizzato, 2. eseguito su dati personali, 3. con lo scopo di valutare aspetti personali di una persona fisica per potervi adattare una determinata reazione. Non si tratta quindi di mero tracciamento dell'interessato, finalizzato alla sola giornalizzazione di eventi, senza uno specifico scopo.

Nel capoverso 10 Si sostituisce la nozione di «organo responsabile» con «titolare dell'elaborazione» al fine di usare la stessa terminologia del Protocollo di emendamento della STE 108 (art. 2 lett. b), della direttiva (UE) 2016/680 (art. 3 n. 8) e del regolamento (UE) 2016/679 (art. 4 n. 7) e infine della nuova LPD. Questa modifica non comporta cambiamenti materiali della nozione. Il titolare del trattamento, come l'organo responsabile, è colui cui competono specifiche decisioni relative all'elaborazione di dati, nella misura in cui il legislatore non abbia già legiferato in materia. Si tratta delle decisioni sulle categorie di dati elaborati, sulle finalità, le modalità del trattamento di dati personali e gli strumenti utilizzati, ivi compreso il profilo della sicurezza. In altre parole, è colui che determina gli obiettivi e i mezzi (trattamento materiale o automatico, software) del trattamento di dati.

Il mandatario è la persona fisica, persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo alla quale viene affidato il compito di trattare dati personali in nome e per conto del titolare dell'elaborazione (capoverso 11). Il contratto che vincola il titolare e il mandatario può essere di varia natura: secondo gli obblighi del mandatario, può trattarsi di un mandato (art. 394 e seguenti CO), di un contratto di appalto (art. 363 e seguenti CO) o di un contratto misto. Il mandatario cessa di essere considerato un terzo dal momento in cui inizia la sua attività contrattuale per conto del titolare del trattamento.

Secondo il capoverso 12 è partecipante la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione o organismo che è autorizzato a inserire i dati personali da esso raccolti, nella banca dati gestita dal titolare del trattamento e a consultare i dati immessi da altri partecipanti. Il diritto del partecipante di immettere dati personali nella banca dati e di consultarli deve essere stabilito nella base legale applicabile alla fattispecie. A titolo di esempio, si può citare la banca dati cantonale sul movimento della popolazione (*movpop*), dove l'organo responsabile è l'Ufficio cantonale del movimento della popolazione e gli organi partecipanti i Comuni, che trasmettono su base regolare i dati del controllo abitanti comunale all'Ufficio cantonale, per verifica dei dati e loro immissione nel *movpop*.

È utente la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che è autorizzato, per legge ad accedere liberamente alla banca dati del titolare del trattamento, per consultarne il contenuto (capoverso 13).

È destinatario di dati la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che riceve dati personali da parte del titolare del trattamento, alle condizioni stabilite dagli articoli 17 e 18 della presente legge (capoverso 14).

È importante, innanzitutto, tenere presente che il consenso è all'ultimo rango dei motivi giustificativi dell'elaborazione previsti dalla LPDP (capoverso 15). Esso va utilizzato in modo eccezionale quando i principali motivi giustificativi (la base legale o la necessità per l'adempimento di un compito pubblico) non sono dati. È pertanto specifico dovere del titolare del trattamento valutare i casi nei quali il consenso possa essere la base giuridica più idonea per il trattamento che intende porre in essere. Il consenso, è definito come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei dati personali che lo riguardano.

Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o a voce. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle (caselle già spuntate).

Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte. Se

il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

Se il titolare decide di basare il trattamento sul consenso deve assicurarsi che esso presenti le seguenti caratteristiche: inequivocabile, libero, specifico, informato, verificabile, revocabile.

1. Consenso inequivocabile vuol dire che non è necessario che sia esplicito ma può anche essere implicito, purché, nel momento in cui sia desunto dalle circostanze, non sussista alcun dubbio che col proprio comportamento l'interessato abbia voluto comunicare il proprio consenso (es. l'inerzia non può costituire manifestazione di consenso, come anche i formulari precompilati e caselle già pre-appuntate). Cioè deve prevedere una chiara azione positiva (come spuntare una casella o inserire la mail in un campo dove è specificata la finalità per la quale sarà usato il dato).
   Il consenso deve, invece, essere esplicito nel caso di trattamento di dati meritevoli di particolare protezione o nel caso di processi decisionali automatizzati (es. profilazione). In altre parole, il consenso inequivocabile può essere dato anche per mezzo di una manifestazione tacita della volontà (cfr. art. 1 del Codice delle Obbligazioni; CO; RS 220). Si è in presenza di una tale manifestazione quando la volontà non si evince da una dichiarazione, bensì da un comportamento che, in base al contesto, può essere interpretato come espressione inequivocabile. Ciò si verifica nel caso di un cosiddetto comportamento concludente, in cui la persona interessata esprime la sua volontà attraverso un determinato atto, ad esempio adempiendo gli obblighi contrattuali. Deve comunque essere espressa una volontà, per cui il silenzio o l'inattività non possono essere considerati un consenso valido per una violazione della personalità. È fatto salvo l'articolo 6 CO, se le parti hanno concordato l'accettazione tacita.
2. Il consenso deve essere dato liberamente, il che significa che l'interessato deve essere in grado di operare una scelta effettiva, senza subire intimidazioni o pressioni, né deve subire conseguenze negative sproporzionate e senza rapporto diretto con l'elaborazione in questione, a seguito del mancato conferimento del consenso. Quando vi è uno squilibrio di potere tra le parti (ad es. tra datore di lavoro e dipendente), la parte ritenuta più debole può dare un consenso valido solo in circostanze eccezionali. Quindi, il consenso non può di principio costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti. In tal caso sarebbe preferibile trattare i dati su base giuridica differente.
3. Il consenso deve essere specifico, cioè relativo alla finalità per la quale è eseguito quel trattamento. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per ogni finalità. Quindi, i dati dovranno essere pertinenti al consenso fornito, e in caso di modifiche del trattamento occorre richiedere un nuovo consenso.
4. Il consenso deve essere informato, occorre cioè che l'interessato sia posto in condizioni di conoscere quali dati sono trattati, con che modalità e finalità e i diritti che gli sono attribuiti dalla legge, cioè deve essere rispettato il principio di trasparenza. Inoltre l'interessato deve essere opportunamente informato sulle conseguenze del suo consenso. L'informazione si ha attraverso l'apposita informativa, che in questo caso diventa una vera e propria condizione di legittimità del trattamento.
5. Consenso verificabile non vuol dire che il consenso deve essere documentato per iscritto, né che è richiesta la forma scritta (anche se in alcune ipotesi, ad es. in caso di elaborazione di dati sensibili, può essere preferibile perché consente più facilmente di

provare il consenso, facilitando quindi le verifiche da parte dell'autorità), ma che chi lo riceve deve essere in grado di dimostrare che l'interessato lo ha conferito.

6. Il consenso deve essere revocabile in qualsiasi momento (fa eccezione il momento inopportuno). La revoca deve essere facile così come lo è dare il consenso. Non vi è alcun obbligo di motivare la revoca, a seguito della quale il trattamento deve interrompersi (ovviamente la revoca non comporta illiceità del trattamento precedente, ma solo l'obbligo di terminare il trattamento), a meno che non sussista una differente base giuridica per continuare il trattamento. Per revocare il consenso, quindi, il titolare dovrebbe predisporre una procedura analoga a quella offerta per concedere il consenso.
   In alternativa è possibile revocare il consenso inviando una comunicazione, o tramite un apposito formulario sul sito, o tramite mail, ai contatti indicati nel sito all'interno dell'informativa. Con la revoca s'innesca inoltre il diritto di cancellazione, per cui il titolare deve cancellare i dati della persona interessata. Ovviamente vi sono motivi legittimi in base ai quali il titolare può avere necessità di conservare alcuni dati della persona interessata anche dopo la revoca del consenso.
   Occorre tenere presente che il consenso non dura per sempre. Quando si raccolgono dati personali occorre informare l'interessato della durata della conservazione (e quindi trattamento) del dato, scaduta la quale il dato va o anonimizzato oppure cancellato.
   Per questo motivo in alcuni casi è preferibile una base giuridica diversa dal consenso.

Articolo 6
Nel capoverso 2 viene adeguata la terminologia, sostituendo il termine di organo responsabile secondo l'attuale articolo 4 capoverso 6 con "titolare dell'elaborazione" (vedi art. 5 cpv. 8). La base legale deve, se del caso, prevedere anche il mandatario (art. 5 cpv. 9).

Per il resto, l'articolo 6 non subisce cambiamenti sostanziali e si rimanda, per il commento, al Messaggio n. 7061 del 18 marzo 2015.

Articolo 7
Si completa la definizione del principio della proporzionalità, aggiungendo a quelli già esistenti della necessità e dell'idoneità, quello della ragionevolezza (o della proporzionalità in senso stretto), vale a dire l'elemento della proporzionalità che prescrive l'esistenza di un rapporto ragionevole tra lo scopo dell'elaborazione e la violazione della personalità che ne risulta (capoverso 3).

Nell'ottica del riordino sistematico della legge, il principio secondo cui la prima fonte di dati personali deve possibilmente essere la persona interessata, viene spostato dall'attuale articolo 9 LPDP nel capoverso 5 dell'articolo 7 concernente i principi.

A proposito del principio dell'esattezza dei dati, che rimane sostanzialmente invariato, è importante sottolineare come esso non venga più attuato unicamente in seguito alla richiesta della persona interessata (diritto di rettifica dei dati, nuovo art. 29), ma anche d'ufficio da parte del titolare dell'elaborazione, in virtù del nuovo articolo 9 (capoverso 6).

La sicurezza dei dati, attualmente prevista all'articolo 17 LPDP, viene ridefinita, aggiungendovi gli scopi perseguiti, vale a dire le garanzie di confidenzialità, integrità e disponibilità dei dati. Trattandosi di un principio della protezione dei dati, la norma è

spostata nel nuovo articolo 7 capoverso 7. Sono toccati dalla norma chiunque elabori dati personali, siano essi titolare, mandatario, partecipante, utente o destinatario secondo l'articolo 5 capoversi 8-12. Per il resto, si rimanda, per il commento all'articolo 7, al Messaggio n. 7061 del 18 marzo 2015.

Articolo 8
La norma sulla responsabilità per la protezione dei dati viene materialmente precisata e adattata nella terminologia (l'organo responsabile diventa il titolare dell'elaborazione, secondo il nuovo articolo 5 capoverso 8). L'attuale capoverso 2 concernente l'obbligo di garantire l'esattezza dei dati viene abrogato, poiché già coperto dal nuovo articolo 7 capoverso 6. Al nuovo articolo 8 capoverso 2 viene aggiunta la data della legge sulla responsabilità civile dello Stato.

L'articolo 21 della direttiva (UE) 2016/680 e l'articolo 26 del regolamento (UE) 2016/679, che prevede una regola analoga, richiamano espressamente la necessità di attribuire in modo trasparente la responsabilità dell'elaborazione dei dati ed in particolare in caso di trattamento congiunto dell'elaborazione dei dati. L'attuale articolo 8 LPDP impone la responsabilità per la corretta elaborazione di dati all'organo che li elabora o che ne demanda l'elaborazione. Conformemente al principio secondo cui la responsabilità per la protezione dei dati segue questi ultimi, essa incombe però non soltanto al titolare dell'elaborazione ma, per le rispettive elaborazioni, a tutta la catena di organi o terzi coinvolti nell'elaborazione dei dati. Così, l'articolo 8 capoverso 1 prevede che anche i partecipanti e/o gli utenti di una banca dati (art. 5 cpv. 10 e 11) e, se del caso, il destinatario di dati (art. 5 cpv. 12) o il mandatario dell'elaborazione (art. 23), sono chiamati ad elaborare i dati di cui dispongono conformemente alla presente legge e ad assumerne la rispettiva responsabilità in caso di violazione. La responsabilità può perciò, nel singolo caso, essere condivisa tra vari attori dell'elaborazione, in funzione dei ruoli assunti. Può essere solidale, quando esiste un rapporto di mandato tra titolare e mandatario dell'elaborazione, oppure quando vi sono più titolari. La responsabilità viene allargata all'obbligo di tutti gli attori coinvolti in un'elaborazione di dati di essere in grado, in ogni momento, di provare che rispettano la protezione dei dati (fardello della prova). Il diritto superiore parla a questo proposito di sistema di gestione della protezione dei dati (SGPD). La prova può essere data ad esempio quando vengono adottati specifici standard di sicurezza, ad esempio le norme ISO relative alla gestione della qualità (ISO 9001) e alla sicurezza dell'informazione (ISO 27001).

Articolo 9
La disposizione prevede che chi tratta dati personali deve accertarsi che siano esatti (obbligo di accertamento). Deve prendere tutte le misure necessarie per rettificare, cancellare o distruggere, d'ufficio, i dati inesatti o incompleti rispetto alle finalità per le quali sono stati raccolti o trattati. I dati che non possono essere rettificati o completati devono essere cancellati o distrutti. La portata dell'obbligo di accertamento va definita di caso in caso e dipende in particolare dalla finalità del trattamento, dalla sua estensione e dal tipo di dati trattati. Se del caso, l'obbligo di accertamento può implicare l'aggiornamento costante dei dati. Determinati obblighi legali possono opporsi alla rettifica, alla cancellazione o all'aggiornamento dei dati. Occorre valutare la questione caso per caso alla luce della finalità dell'elaborazione. In riferimento all'attività di archivi, musei, biblioteche e altre istituzioni della memoria collettiva, il principio di esattezza e gli obblighi connessi devono essere giudicati in modo differenziato. Gli archivi hanno infatti il compito

di rappresentare, per mezzo di documenti, un'immagine momentanea del passato la cui «esattezza» va giudicata unicamente in riferimento alla rappresentazione fedele dei documenti stessi.

Il titolare dovrà comunicare le eventuali correzioni ai destinatari cui i dati siano stati trasmessi, a meno che risulti essere impossibile o implichi uno sforzo sproporzionato. Inoltre, in presenza di una richiesta dell'interessato, il titolare del trattamento gli dovrà comunicare informazioni relative a tali destinatari.

Articolo 10
Fra i principi che reggono l'elaborazione di dati personali vi è l'obbligo di informare le persone interessate in occasione della raccolta di dati. Tale obbligo costituisce una concretizzazione del principio di buona fede di cui all'articolo 9 Cost./CH Nella LPDP il principio è ancorato all'articolo 7 capoverso 2.

In quest'ottica l'obbligo di informare implica che l'informazione sia chiara, possibilmente esaustiva e non contraddittoria. L'obbligo sussiste soprattutto laddove i dati non siano raccolti presso la persona interessata. L'obbligo di informare costituisce inoltre un'attuazione del principio di trasparenza dell'attività amministrativa. L'informazione migliora la qualità dei rapporti tra lo Stato e il cittadino e rafforza la consapevolezza della persona interessata circa i suoi diritti. Senza la necessaria informazione, quest'ultima potrebbe non venire a sapere che i suoi dati vengono trattati.

Questa trasparenza e questa sensibilizzazione costituiscono obiettivi fondamentali perseguiti non solo dalla LPDP ma anche dalla nuova LPD (cfr. Messaggio n. 17059, pag. 6039). L'articolo 10 è meno articolato rispetto alla soluzione proposta dal legislatore federale; quest'ultimo ha infatti previsto obblighi d'informazione più estesi (cfr. art. 17 cpv. 4 e 5 nuova LPD). Con l'obbligo di informare vi è del resto un generale allineamento alla Direttiva UE 2016/680, al Protocollo di emendamento della STE 180 e alle raccomandazioni che la Conferenza dei Cantoni ha emesso in vista dell'adeguamento delle leggi cantonali sulla protezione dei dati al diritto internazionale.

La norma sancisce innanzitutto il principio dell'obbligo di informare. La disposizione esige che il titolare dell'elaborazione, ovvero colui che determina le finalità e i mezzi dell'elaborazione di dati personali, informi la persona interessata su ogni raccolta di dati personali. L'obbligo è volto principalmente ad evitare che vengano raccolti dati all'insaputa della persona.

La norma non precisa in che modo e in che forma debba essere comunicata l'informazione. In assenza di ulteriori precisazioni nel regolamento di applicazione, il titolare del trattamento potrà scegliere le modalità ritenute più consone ed efficaci. È sicuramente preferibile un'informazione mirata e individuale mediante invio personale scritto o tramite e-mail ma, a dipendenza del numero o delle categorie di persone interessate, non sono da escludere anche altre modalità o vie di comunicazione, ad esempio un'informativa generale concernente tutti i funzionari da pubblicare sul sito intranet dell'amministrazione pubblica, o un'informativa generale concernente tutti gli allievi di un determinato istituto da pubblicare all'albo della scuola. Ciò che importa è che il modo e la forma utilizzati consentano di raggiungere tutte le persone interessate e di principio solo quelle. Non è

necessario che il titolare del trattamento accerti che tali persone abbiano effettivamente preso atto dell'informazione portata a loro conoscenza.

Il momento della comunicazione deve coincidere fondamentalmente con quello della raccolta dei dati.

Con l'introduzione di questa norma si raggiunge un generale allineamento al disegno di legge della LPD.

In seguito, la norma descrive il contenuto minimo dell'informazione. La frase introduttiva prevede che al momento della raccolta, il titolare dell'elaborazione, comunichi all'interessato le informazioni indispensabili, affinché quest'ultimo possa fare valere i suoi diritti e sia garantita la trasparenza dell'informazione. A tal fine occorre pertanto che l'informazione sia comprensibile e corretta. Rimane riservato il diritto speciale, ad esempio in materia di polizia.
Le lettere a-g della norma indicano quali informazioni minime debbano essere concretamente fornite alla persona interessata.

La lettera a) dispone che il titolare dell'elaborazione comunichi l'identità (il cognome e nome) e le coordinate di contatto del titolare dell'elaborazione (per es. indirizzo, indirizzo e-mail, numero di telefono).

La lettera b) è volta a chiarire le finalità dell'elaborazione dei dati: essa prevede infatti che l'informazione indichi lo scopo della raccolta di dati e anche la base legale, laddove esiste. L'articolo 6 esige, infatti, una base legale formale o materiale per tutte le elaborazioni sistematiche, non invece per quelle nel singolo caso.

Anche l'eventuale cambiamento dello scopo della raccolta dev'essere comunicato al diretto interessato (lett. c).

La lettera d) statuisce che il titolare del trattamento comunica i dati o le categorie di dati elaborati. Per dati occorre intendere tutti i dati, inclusi quelli meritevoli di particolare protezione. Le categorie di dati possono essere molteplici e concernere ad es. la salute, la formazione, i titoli di studio, i provvedimenti, ecc.

Il titolare del trattamento è tenuto a informare i diretti interessati anche in caso di trasmissione di dati a organi pubblici o a persone private secondo quanto previsto dagli articoli 10 e 11. La lettera e) sancisce infatti che il titolare del trattamento comunica, se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali.

La persona interessata deve inoltre essere resa edotta circa i suoi diritti (lett. f).

I diritti sono quelli definiti dagli articoli 27 e seguenti e consistono sostanzialmente nella consultazione dei registri, nel diritto di chiedere informazioni in merito all'elaborazione di dati che la riguardano, nel diritto di rettifica, di blocco e d'interruzione di un'elaborazione di dati.
Il titolare comunica inoltre, solo su richiesta del diretto interessato, tutte le altre informazioni complementari necessarie a garantire un'elaborazione corretta e trasparente dei dati personali (lett. g).

Le lettere d-f del capoverso 2 si allineano con quando prevede il protocollo di emendamento STE 180.

Articolo 11
L'obbligo d'informazione si estende ai casi in cui è intervenuta una rettifica, cancellazione o distruzione di dati, nonché una limitazione della loro elaborazione. Tali eventi possono essere intervenuti sia a seguito dell'esercizio dei diritti delle persone previsti dai nuovi articoli 27 e seguenti, oppure a seguito di una loro modifica o limitazione d'ufficio. L'informazione serve ad evitare che i dati continuino ad essere elaborati in modo non aggiornato da parte dei destinatari. L'informazione qui disciplinata è rilevante in particolare nei casi in cui i dati non vengono trasmessi tramite procedura di richiamo. Se invece i destinatari possono accedere a una banca dati tramite procedura di richiamo, essi sono già informati in tempo reale delle modifiche o limitazioni intervenute. L'informazione concernente le modifiche intervenute in una banca dati non deve necessariamente avvenire ad ogni singola modifica, ma è sufficiente informare l'utenza a scadenze regolari.

Articolo 12
Il capoverso 1 definisce le situazioni in cui il titolare del trattamento non ha obbligo di informazione nei confronti della persona interessata. Sono i casi in cui l'informazione è sostanzialmente superflua, non necessaria, poiché la persona interessata è già aggiornata, oppure quando l'informazione è impossibile o richiede mezzi sproporzionati. Secondo quanto prevede la lettera a) l'obbligo decade se la persona interessata dispone già delle pertinenti informazioni di cui all'articolo 10. È possibile ipotizzare il caso in cui la persona interessata sia già stata in precedenza informata e che in seguito le informazioni da comunicare non siano cambiate.

La lettera b) dispone che non vi è obbligo di informare quando l'elaborazione dei dati personali è prevista dalla legge. Ad esempio, non sarà necessario informare i dipendenti dello Stato sull'elaborazione di dati personali necessari alla gestione del personale e degli stipendi, perché in materia esiste una chiara base legale (cfr. art. 84 e seguenti LORD).

Non vi è infine obbligo di informare se l'informazione è impossibile o esige mezzi sproporzionati (lett. c). L'informazione è impossibile se la persona interessata, nonostante tutte le ricerche ragionevolmente esigibili, rimane sconosciuta o non è identificabile.

L'informazione esige mezzi sproporzionati, quando gli sforzi messi in atto appaiono del tutto inadeguati in relazione ai benefici per la persona interessata. Analogamente a quanto indicato a livello federale "l'informazione necessita ad esempio di sforzi sproporzionati quando i dati sono trattati unicamente per scopi di archiviazione d'interesse pubblico.

In tal caso l'informazione di tutte le persone interessate richiederebbe regolarmente sforzi notevoli ed è probabile che l'interesse di queste ultime all'informazione sia limitato, ad esempio perché i dati in questione sono vecchi" (vedi Messaggio del 15 settembre 2017, FF 2017 5939, 6042).

La norma prevede inoltre che l'informazione in occasione della raccolta di dati personali alla persona interessata possa essere limitata o rifiutata alle stesse condizioni previste per il diritto di accesso. L'informazione può essere limitata o rifiutata quando interessi pubblici

preponderanti (ad esempio per motivi di sicurezza interna) o interessi di terzi particolarmente meritevoli di protezione lo esigono, oppure quando la comunicazione dell'informazione potrebbe compromettere la finalità della raccolta. In tutti questi casi la decisione dipende da un'accurata ponderazione degli interessi in gioco. Elementi di ponderazione sono principalmente il tipo di dati trattati (sensibili o meno sensibili), il modo in cui sono trattati, il rischio di lesione di diritti della persona, l'importanza dello scopo del trattamento, la misura in cui l'informazione della persona ostacola il raggiungimento dello scopo del trattamento.

Articolo 13
Il diritto superiore (art. 8bis cifra 2 STE 108 e art. 27 e seguenti della direttiva (UE) 2016/680) impone una valutazione d'impatto da parte dell'organo pubblico responsabile per i progetti di elaborazione di dati che verranno inizializzati dopo l'entrata in vigore della presente revisione. La valutazione d'impatto rappresenta uno strumento per riconoscere e valutare i rischi che una determinata elaborazione può comportare per la persona interessata. Sulla base di tale valutazione vanno, se del caso, presi i provvedimenti necessari per ridurre tali rischi. La valutazione d'impatto permette inoltre al titolare dell'elaborazione di affrontare preventivamente eventuali problemi di protezione dei dati e di evitare costi successivi. La valutazione d'impatto deve essere effettuata quando esiste un rischio elevato per la personalità e i diritti fondamentali, indipendentemente dal fatto che esista o meno una base legale per l'elaborazione in questione. Vanno quindi valutati il modo e la misura in cui un trattamento si ripercuote sulla personalità e i diritti fondamentali (in particolare, sul diritto all'autodeterminazione e sulla sfera privata). Occorre di principio presumere un rischio elevato quando le caratteristiche specifiche del trattamento inducono a concludere che esso limiti o potrebbe limitare la libertà della persona interessata di disporre dei propri dati. Il rischio elevato può risultare ad esempio dal tipo di dati trattati o dal loro contenuto (ad esempio, dati meritevoli di particolare protezione), dal tipo e dallo scopo dell'elaborazione (per esempio, profilazione), dalla quantità dei dati elaborati, dalla loro comunicazione all'estero (per esempio, in Stati senza protezione equivalente) o dai diritti di accesso ai dati. In ogni caso, se l'elaborazione è sistematica, se i dati sono meritevoli di particolare protezione e se gli scopi dell'elaborazione sono ampi, allora occorre concludere che il rischio è elevato.
Esempi di elaborazione a rischio elevato possono essere riconosciuti segnatamente nella videosorveglianza invasiva di luoghi pubblici, nel settore medico e nella profilazione.

La valutazione d'impatto è, peraltro, un elemento della prova che il titolare del trattamento rispetta la protezione dei dati secondo il nuovo articolo 8 capoverso 1. L'analisi deve indicare in particolare i vari processi (p. es. la tecnologia usata), lo scopo del trattamento e la durata di conservazione dei dati, i vari rischi per i diritti delle persone interessate e le misure per ridurli. È un documento utile nell'ambito della consultazione preventiva secondo il nuovo articolo 15.

Articolo 14
Per quanto riguarda il principio della protezione dei dati sin dalla progettazione, si fa qui di seguito riferimento a quanto riportato dai materiali legislativi federali della revisione della legge federale sulla protezione dei dati, poiché la questione è identica.

Sulla base del primo capoverso, il titolare dell'elaborazione è tenuto ad adottare, fin dalla progettazione del trattamento, le misure appropriate per attuare le disposizioni sulla

protezione dei dati. Il progetto di nuova LPDP introduce pertanto il principio della protezione dei dati fin dalla progettazione (privacy by design). L'idea alla base della protezione fin dalla progettazione è che la tecnica e il diritto si completino a vicenda. Una tecnica favorevole alla protezione dei dati permette di ridurre la necessità di regole giuridiche (o di codici di condotta), in quanto gli accorgimenti tecnici rendono impossibile una violazione della protezione dei dati o perlomeno ne riducono notevolmente il rischio. Nel contempo le tecnologie che favoriscono la protezione dei dati sono imprescindibili per l'applicazione delle disposizioni sulla protezione dei dati. Infatti, il trattamento di dati è un fenomeno onnipresente e tenderà ancora ad aumentare. Ne consegue un'innumerevole quantità di dati che devono essere trattati conformemente alle regole sulla protezione dei dati. A tal fine gli accorgimenti tecnici sono d'importanza fondamentale. In generale, la protezione dei dati fin dalla progettazione non è legata a una determinata tecnologia. Si tratta piuttosto di progettare, sotto il profilo tecnico e organizzativo, i sistemi per l'elaborazione dei dati in modo tale da conformarli in particolare ai principi della protezione dei dati. In altre parole, il sistema deve attuare i requisiti per un'elaborazione dei dati conforme alla legge in modo tale da ridurre o escludere il rischio di violazioni delle disposizioni sulla protezione dei dati. È ad esempio possibile impostare un sistema di modo che i dati siano cancellati a intervalli regolari o anonimizzati in maniera standardizzata. Per la protezione fin dalla progettazione è d'importanza particolare che i dati raccolti siano ridotti al minimo indispensabile, affinché sia rispettato il principio della proporzionalità. Sin dall'inizio, l'elaborazione deve essere pertanto progettata in modo tale da raccogliere e trattare il minor numero possibile di dati o perlomeno in modo tale da doverli conservare meno tempo possibile.

Il capoverso 2 precisa i requisiti posti ai provvedimenti di cui al capoverso 1: devono essere adeguati in particolare allo stato della tecnica, alla natura e all'estensione dell'elaborazione dei dati come pure al grado di probabilità e di gravità del rischio che l'elaborazione implica per la personalità e i diritti fondamentali della persona interessata. La disposizione si basa su un approccio basato sui rischi. Il rischio che consegue da un'elaborazione deve essere messo in relazione con le possibilità tecniche di ridurlo. Quanto più alto è il rischio e la probabilità che si verifichi e quanto più ampia è l'elaborazione di dati, tanto più elevati dovranno essere i requisiti posti ai provvedimenti tecnici, affinché siano da ritenersi adeguati ai sensi della presente disposizione.

Articolo 15

L'articolo 28 della Direttiva (UE) 2016/680 prescrive di sottoporre determinati progetti di elaborazione di dati all'Incaricato per una consultazione preventiva (preavviso). Si tratta di progetti legislativi o di progetti per i quali la valutazione d'impatto (art. 13) ha rilevato dei rischi elevati per i diritti e le libertà della persona, oppure di progetti per i quali il tipo di elaborazione (segnatamente, nuovi meccanismi, tecnologie o procedure) presentano dei rischi elevati. Si può citare, a titolo d'esempio, il progetto Rapporto sociale dell'Ufficio di statistica per la realizzazione di uno strumento per il monitoraggio sociodemografico ed economico della popolazione, che prevede di collegare dati di natura diversa, (amministrativi, fiscali, statistici), sulla base degli identificatori univoci dell'individuo (numero AVS) e dell'edificio/abitazione (numero EGID/EWID), oppure progetti di ampliamento della videosorveglianza del demanio pubblico. Anche i progetti legislativi che toccano alla protezione dei dati vanno sottoposti all'Incaricato.

La consultazione preventiva permette all'Incaricato di intervenire a titolo preventivo e di consulenza, permettendo di risolvere eventuali problemi di protezione dei dati in una fase precoce del progetto. La nuova norma rafforza l'attuale articolo 18 capoverso 2 LPDP concernente l'informazione dell'Incaricato circa la messa in opera di elaborazioni di dati che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone.

Di principio, i preavvisi non hanno conseguenze giuridiche dirette sulla situazione di terzi e non costituiscono delle decisioni, ma sono considerati come degli atti interni. In quanto tali, non sono suscettibili di ricorso. Se sono ripresi in una decisione preavvisata, il loro contenuto può essere contestato in un ricorso contro la stessa. I preavvisi non legano l'autorità che li riceve, anche se quest'ultima avrà spesso tendenza a seguirli, visto il carattere sovente tecnico degli stessi. Se l'autorità è obbligata per legge a richiedere un preavviso, nel caso in cui se ne distanzia nella sua decisione deve motivare la sua posizione, per dimostrare che ha dei motivi pertinenti per decidere in tal senso.

I criteri per la ripresa di progetti nella lista di progetti da sottoporre preventivamente all'Incaricato vanno stabiliti dal Consiglio di Stato (capoverso 2). Essi sono, ad esempio, la cerchia di persone interessate, il numero di organi partecipanti, la sensibilità dei dati (art. 28 cpv. 3 Direttiva (UE) 2016/680).

Articolo 16
Le violazioni della protezione dei dati devono essere notificate senza ritardo all'Incaricato, a meno che la violazione non presenti verosimilmente nessun rischio per la personalità e i diritti fondamentali delle persone interessate. Il contenuto della notifica è disciplinato nelle norme materiali d'esecuzione, e possono ad esempio essere i dettagli della violazione, gli effetti probabili sulla persona e le misure effettive previste per ristabilire la protezione dei dati e attenuare gli effetti della violazione. L'organo pubblico responsabile informa inoltre le persone interessate quando le circostanze lo esigono (ad esempio, in caso di grave e/o imminente rischio per la personalità delle persone interessate) o quando l'Incaricato lo richiede. L'informazione è obbligatoria quando le persone interessate possono prendere le misure necessarie per evitare un pregiudizio. L'organo pubblico può rinunciare all'informazione se prende delle misure che con tutta probabilità eliminano i rischi. Può rinunciare all'informazione pure se un interesse pubblico o privato preponderante lo esige. Se la violazione ha luogo nell'ambito di un mandato di elaborazione di dati (nuovo art. 23), il mandatario la notifica senza indugio al titolare dell'elaborazione, che la segnalerà in seguito all'Incaricato.

La notifica di una violazione della protezione dei dati può, se del caso, portare a una raccomandazione o decisione dell'Incaricato (art. 38).

Capitolo quarto
Nel capitolo riguardante la trasmissione di dati personali da rilevare innanzitutto lo spostamento degli articoli 12 e 13 LPDP nella legislazione sull'armonizzazione dei registri e sul controllo abitanti.

Articolo 17
L'articolo 17 è una norma di valenza generale e prevede, per la trasmissione di dati a organi pubblici, tre possibili motivi giustificativi: La legge settoriale (lett. a), la necessità dei

dati per l'adempimento di compiti legali (lett. b), il consenso della persona interessata (lett. c).

Il motivo giustificativo della legge settoriale (lett. a) è necessario nel caso di trasmissioni sistematiche di dati personali, in virtù dell'obbligo della base legale per elaborazioni sistematiche (art. 6 LPDP). Se il diritto settoriale secondo l'articolo 17 lettera a) LPDP non disciplina la trasmissione di dati, l'organo interessato può avvalersi, limitatamente alla trasmissione di dati nel singolo caso, degli altri due motivi giustificativi previsti all'articolo 17 lettere b) e c) LPDP. I compiti legali secondo la lettera b) devono essere esplicitamente previsti oppure devono perlomeno essere chiaramente deducibili dalla legge applicabile. Dal canto suo, per essere giuridicamente vincolante, il consenso secondo l'articolo 17 lettera c) deve adempiere alle condizioni poste dall'articolo 5 capoverso 14.

Se il diritto settoriale riservato all'articolo 17 lettera a) disciplina una determinata trasmissione di dati personali, si pone la questione a sapere se i restanti motivi giustificativi generali previsti dall'articolo 17 lettere b e c LPDP rimangono, concorrentemente, applicabili.

Per dirimere questo quesito va – in primo luogo e in ogni singolo caso – interpretata la volontà del legislatore del diritto settoriale, applicando i metodi classici d'interpretazione del diritto (tra i quali, l'interpretazione letterale, logica, sistematica, teleologica, storica e analogica) e tenendo conto dei principi e dei diritti fondamentali della protezione dei dati, in particolare il diritto all'autodeterminazione informativa. Secondo quanto precede, il consenso della persona interessata può, di principio, giustificare una trasmissione di dati che travalica quanto disposto dal diritto settoriale riguardo la trasmissione di dati. Possono essere d'ausilio, in secondo luogo, pure i principi *lex specialis derogat legi generali, lex posterior derogat legi priori* e *lex superior derogat legi inferiori,* i quali hanno tuttavia una valenza relativa, segnatamente quando entrano in conflitto tra di loro (ad esempio, quando, sullo stesso oggetto, a una norma di diritto speciale anteriore fa seguito una norma di diritto generale superiore).

La trasmissione di dati, rispettivamente l'assistenza amministrativa tra organi pubblici secondo l'articolo 17 lettere a) e b), solleva anche la questione della liceità della trasmissione - a autorità che ne fanno richiesta (autorità richiedenti) - di dati e documenti emessi da autorità terze (autorità emittenti) e in possesso dell'autorità cui è rivolta la richiesta (autorità detentrice). Si tratta, in altre parole, della questione della responsabilità per la valutazione dell'adempimento delle condizioni per la trasmissione di dati e, se del caso, per la rispettiva trasmissione. Il quesito va risolto affermativamente, nel senso che l'autorità detentrice va considerata come responsabile di tali valutazioni e ponderazioni, in particolare per quanto riguarda i compiti legali e le rispettive necessità informative addotte dall'autorità richiedente. Se lo ritiene necessario o opportuno, l'autorità detentrice può sempre richiedere un parere all'autorità emittente, oppure può richiedere il consenso per la trasmissione alla persona interessata. Nel caso in cui l'autorità detentrice conclude che un determinato documento di una terza autorità non vada trasmesso, può comunque sempre segnalarne l'esistenza e la rispettiva autorità emittente all'autorità richiedente.

Articolo 18

Alla stessa stregua di quanto previsto per la trasmissione a organi pubblici, anche nella trasmissione di dati a persone private viene richiamato, al capoverso 1 lettera a), il diritto settoriale, per garantire la sicurezza giuridica quanto al rapporto tra quest'ultimo e la LPDP.

Per quanto riguarda il campo di applicazione, al capoverso 1 lettera b) viene sostituito il concetto di accessibilità dei dati "a chiunque" con "pubblicamente". Con questa precisazione è più chiaro che la norma copre qualsiasi divulgazione o pubblicazione di propri dati personali, quindi non soltanto quelle destinate potenzialmente a tutto il mondo (ad esempio, tramite un sito internet o un profilo di Social media con utenza illimitata o aperta), ma anche le pubblicazioni circoscritte a un pubblico o a un gruppo di persone più ristretto (ad esempio, tramite l'albo comunale, un giornale cartaceo locale, una trasmissione radiofonica o televisiva locale oppure un profilo di social media con cerchia di utenza limitata).

In ogni caso, la trasmissione a persone private secondo l'articolo 18 capoverso 1 deve tenere conto dei principi generali della protezione dei dati, in particolare dei principi della proporzionalità e della finalità, e tenere anche adeguatamente conto delle finalità perseguite dalla persona interessata e ragionevolmente deducibili dal contesto. In particolare, secondo il principio della finalità, i dati resi pubblici dalla persona interessata non sono in seguito liberamente trasmissibili a terzi, anche se la persona interessata non ha espresso un formale diniego alla trasmissione a terzi non autorizzati Occorre, in altre parole, che la trasmissione da parte del titolare rientri nelle finalità perseguite dalla persona interessata quando ha reso pubblici i suoi dati.

Per il resto, la norma sulla trasmissione di dati a privati non prevede più, come è ancora il caso con l'attuale articolo 11, la trasmissione di dati contenuti in pubblicazioni ufficiali (cpv. 3) e la trasmissione per indirizzari e pubblicazioni simili d'interesse generale (cpv. 4).

Queste norme sono abrogate, poiché devono essere disciplinate nel rispettivo diritto settoriale (ad esempio, nella legislazione cantonale sulle pubblicazioni ufficiali per la trasmissione di dati secondo l'articolo 11 capoverso 3, e, per quanto riguarda le trasmissioni secondo l'articolo 11 capoverso 4, nella legge federale sulla circolazione stradale per l'elenco delle targhe automobilistiche, o nel diritto sulla navigazione per le targhe dei natanti). In particolare l'attuale capoverso 4, teneva conto del fatto che in più Cantoni, anni fa, si trovavano in commercio varie pubblicazioni di interesse generale praticate da aziende private quali indirizzari, elenchi dei detentori di veicoli a motore (CD-ROM Autodex, ecc.) o di natanti, ecc. La trasmissione dei dati da parte del Cantone a queste aziende necessitava, secondo l'articolo 11 capoverso 4 LPDP, di norme che andavano oltre a quanto allora previsto dalla legge, vale a dire di una convenzione (art. 11 RLPDP; vedi anche Messaggio governativo n. 2975 del 2 ottobre 1985, commento ad art. 11 cpv. 3 pag. 9). Oggi questi indirizzari sono disciplinati dal diritto settoriale, il quale prevede ad esempio la pubblicazione delle targhe automobilistiche (LCStr) e dei natanti esclusivamente da parte del Cantone (e non più anche di aziende private), così come degli indirizzari e numeri di telefono dei vari fornitori di servizi di telecomunicazione (Ordinanza federale concernente local.ch). Per questo motivo, la norma non ha più una ragione di essere e va abrogata.

Articolo 19
La norma di coordinamento con la legge sull'informazione e sulla trasparenza dello Stato (LIT; RL 162.100), attualmente posizionata all'articolo 11 capoverso 2 (trasmissione di dati a privati), diventa una norma a sé stante (art. 19). Secondo tale norma, se l'informazione conformemente all'articolo 5 LIT comprende dati personali, l'interesse generale alla loro pubblicazione deve prevalere rispetto alla protezione dei dati e la loro pubblicazione deve essere in rapporto con l'adempimento di compiti pubblici (art. 19 lett. a). La pubblicazione di dati personali deve comunque in ogni caso rispettare i principi generali della protezione dei dati, in particolare i principi della finalità, della proporzionalità e dell'esattezza dei dati (art. 7). Da notare che per trasmissione di dati personali d'ufficio secondo s'intende quella avente luogo in virtù di una norma di diritto settoriale.

Articolo 20
La norma rimane sostanzialmente immutata.

Articolo 21
Il capoverso 1 precisa, ora, che una delle condizioni cui può essere assoggettata una trasmissione consiste nella sottoscrizione di una convenzione sulla protezione dei dati. La convenzione è disciplinata nel dettaglio all'attuale articolo 10 del regolamento d'esecuzione della LPDP.

Per il resto, è importante precisare che, per quanto riguarda il campo di applicazione dell'articolo 21 capoverso 1, esso si applica a tutte le trasmissioni di dati, salvo quelle che avvengono in virtù di un obbligo legale alla trasmissione di dati (vale a dire fondate su una base legale imperativa conforme ai dettami dell'articolo 6 capoverso 3 LPDP), oppure in virtù del consenso libero e informato della persona interessata. La norma si applica perciò alle trasmissioni fondate su basi legali potestative (ad esempio, l'articolo 22 concernente la trasmissione per elaborazioni senza riferimento a persone specifiche), oppure a quelle che avvengono in seguito a comprovate necessità dell'organo richiedente per l'adempimento dei suoi compiti legali (art. 17 lett. b).

Il terzo capoverso concernente l'obbligo della base legale per l'accesso a dati personali mediante una procedura di richiamo (art. 14 cpv. 4) viene abrogata, poiché già coperta dall'articolo 6 capoverso 1 concernente l'obbligo della base legale per elaborazioni sistematiche di dati personali.

Articolo 22
La norma sull'elaborazione senza riferimento a persone specifiche (attuale art. 15 LPDP) viene, innanzitutto, adeguata terminologicamente, nel senso che l'organo responsabile previsto al capoverso 1 diventa il titolare dell'elaborazione (art. 5 cpv. 8). Per garantire una maggiore chiarezza giuridica, il primo capoverso viene, inoltre, riformulato, sostituendo il passaggio "senza riferimento a persone specifiche" con "per scopi impersonali". Infatti, l'attuale formulazione, che prevede tra l'altro la trasmissione di dati personali senza riferimento a persone specifiche, è contraddittoria: al momento della loro trasmissione per elaborazioni senza riferimento a persone specifiche, i dati fanno di principio ancora riferimento a persone specifiche. Con la nuova formulazione, questa imprecisione viene eliminata.

Alla stessa stregua di quanto previsto per l'elaborazione su mandato (art. 23), viene aggiunto un nuovo capoverso 2 che prevede l'obbligo della sottoscrizione di una convenzione sulla protezione dei dati in caso di trasmissione di dati a scopi impersonali.

L'articolo 15 capoverso 2 viene spostato nell'articolo 22 capoverso 3 e modificato in tal modo da chiarire che quando i dati sono anonimizzati in modo definitivo, la loro elaborazione non sottostà più a tutta la LPDP (attualmente, invece, l'articolo 15 capoverso 2 LPDP prevede che se i dati sono elaborati senza riferimento a persone specifiche non si è più tenuti a osservare la compatibilità degli scopi (art. 6 cpv. 3) e i limiti imposti alla trasmissione (art. 10 e 11).

Articolo 23
Viene aggiunto un nuovo capoverso 1 che precisa che il mandato di elaborazione di dati non può avvenire se ciò è esplicitamente escluso dal diritto. Inoltre, la norma viene adattata terminologicamente, sostituendo il termine "organo responsabile" con "titolare dell'elaborazione" (art. 5 cpv. 8).

I capoversi 2 e 3 riprendono l'attuale articolo 16 capoversi 1 e 2 LPDP, senza variazioni sostanziali. Si precisa a proposito del capoverso 3 che l'autorizzazione derogante è necessaria anche per il sotto-mandato.

Articolo 24
Quando occorre avviare un trattamento di dati personali spesso ci si trova confrontati con l'incertezza sulle modalità più appropriate della sua attuazione sia dal punto di vista dell'efficienza dei processi sia da quello della protezione dei dati trattati. Le novità tecniche, i mezzi a disposizione, le interconnessioni tra le attività e le banche di dati degli uffici eccetera a volte rendono difficile l'elaborazione di una base legale in senso formale perché non sempre le implicazioni sono prevedibili in anticipo. Per queste ragioni, il messaggio propone l'introduzione di una norma che consenta al Consiglio di Stato di autorizzare il trattamento di dati personali mediante un decreto esecutivo. Prima dell'eventuale rilascio di un'autorizzazione il Consiglio di Stato chiede un parere all'Incaricato.

L'organo responsabile presenta al Consiglio di Stato entro due anni dall'avvio del trattamento dei dati un rapporto di valutazione del progetto pilota. Il rapporto propone l'interruzione del trattamento o la sua continuazione. In questa ultima ipotesi, l'organo responsabile può proporre degli adeguamenti al progetto.

L'assenza di una base legale adottata dal Gran Consiglio ha carattere temporaneo. Infatti, l'articolo proposto stabilisce che la regolamentazione del Consiglio di Stato decade al più tardi dopo cinque anni dall'avvio del trattamento. Quindi la continuazione del trattamento oltre il termine di cinque anni è ammessa solo se entro quel termine è entrata in vigore la base legale formale. Il Consiglio di Stato non ha la facoltà di prorogare quel termine. Poiché il processo legislativo di adozione di una legge comprende la possibilità di sottoporre una legge a una votazione popolare mediante referendum, l'uso di questo strumento non può comportare un allungamento del termine ma deve essere considerato nel processo legislativo. Una proroga può essere ipotizzata invece nel caso di un ricorso al Tribunale federale contro l'atto legislativo.

La norma proposta si ispira a norme analoghe del diritto federale e di alcuni Cantoni. Si tratta in particolare dell'articolo 35 della LPD del 25 settembre 2020 e dell'articolo 12f della *loi sur la protection des données* del 25 novembre 1994 (LPrD, RSF 17.1).

Articolo 25
Oltre all'adattamento terminologico ("l'organo responsabile" diventa "titolare dell'elaborazione"), la norma sulla conservazione, archiviazione e distruzione dei dati viene formalmente e materialmente modificata. Innanzitutto – tenendo conto delle prescrizioni dettate dall'articolo 6 capoverso 2 LPDP in materia di obblighi legislativi – il nuovo articolo 25 capoverso 1 prevede che sia sempre il legislatore, e non più anche, in determinate circostanze, il titolare dell'elaborazione a definire lo scopo, le modalità e la durata di conservazione dei dati (vedi attuale art. 21 cpv. 2 LPDP). Oltre a tale cambiamento di competenze normative, il nuovo articolo 25 capoverso 1 assorbe e condensa anche i capoversi 1 e 4 dell'attuale articolo 21 LPDP. Da un lato, quindi, si stabilisce che il legislatore, nella definizione della conservazione dei dati, deve tenere conto dei principi della necessità e della finalità dei dati in ambito di conservazione (ivi comprese eventuali necessità di conservazione delle persone interessate). Dall'altro, il nuovo capoverso 1 attribuisce al legislatore la competenza legislativa in materia di modalità di conservazione dei dati (attuale art. 21 cpv. 4 LPDP). In altre parole, tutte le necessità di utilizzazione e di prova, ivi comprese le eventuali esigenze di conservazione a tutela di interessi degni di protezione della persona interessata, devono consumarsi entro il termine di conservazione dei dati stabilito dal legislatore per l'archiviazione intermedia presso il titolare dell'elaborazione. Scaduto il termine di conservazione, i dati vanno proposti all'Archivio di Stato, che ne determina il valore archivistico (art. 5 cpv. 3 della legge sull'archiviazione e sugli archivi pubblici del 15 marzo 2011; LArch; RL 164.100 e art. 9 del regolamento della legge sull'archiviazione e sugli archivi pubblici del 28 marzo 2012; RLArch; RL 164.110). Presso il detentore dei dati, essi possono essere conservati oltre il termine di conservazione unicamente ancora in forma anonima per scopi statistici, di ricerca o per altri scopi impersonali.

Articolo 26
Il diritto superiore sostituisce il registro delle banche dati con quello delle elaborazioni di dati. Poiché con il concetto di elaborazione di dati personali s'intende ogni operazione intesa, segnatamente, a raccogliere, registrare, utilizzare, modificare, trasmettere, cancellare, conservare o distruggere questi dati (art. 5 cpv. 3), appare evidente che l'iscrizione a registro di tutte queste operazioni risulterebbe estremamente onerosa per gli organi pubblici interessati. Poiché lo scopo di trasparenza che il diritto superiore intende perseguire è però già in buona parte raggiunto con i nuovi obblighi d'informazione delle persone interessate in occasione della raccolta di dati personali (art. 10) e in occasione della rettifica, cancellazione o distruzione di dati (art. 11) e ritenuto che con il concetto di banca dati si intendono anche quelle non strutturate (art. 5 cpv. 7), il presente disegno di legge rinuncia a estendere l'obbligo di iscrizione nel registro a tutte le elaborazioni di dati, e mantiene l'attuale impostazione, limitata all'iscrizione dei soli archivi di dati.

L'articolo 26 condensa gli attuali articoli 19 e 20 LPDP sui registri dei titolari delle elaborazioni e sul registro centrale dell'Incaricato, poiché sostanzialmente uguali. Considerato che i registri sono pubblici (art. 26 cpv. 3), va da sé che chiunque possa consultarli. Per questo motivo l'attuale articolo 22 concernente la consultazione dei registri risulta superfluo.

La delega del disciplinamento delle norme materiali al Consiglio di Stato è ripresa nel nuovo articolo 43 lettera h concernente le disposizioni esecutive.

Queste ultime disciplineranno, tra l'altro, anche le eccezioni all'obbligo di iscrizione a registro, che potranno eventualmente completare, rispettivamente differire da quelle attualmente previste all'articolo 19 capoverso 3 LPDP.

Articolo 27
Il diritto di accesso è uno dei pilastri principali della protezione dei dati. È la condizione che permette l'esercizio degli altri diritti della persona e la loro attuazione in giustizia, in particolare del diritto di rettifica di dati inesatti o incompleti, del diritto di blocco della loro trasmissione e del diritto di interruzione della loro elaborazione illecita. Al capoverso 1 vengono riprese, sotto forma di elenco, le condizioni dell'attuazione di una richiesta di diritto di accesso. Le condizioni sono completate con la necessità di fornire le informazioni entro un termine ragionevole e, di principio, gratuitamente. Essendo emanazione della protezione costituzionale della personalità, il diritto di accesso non deve essere motivato e non può, di principio, essere legato a costi del suo esercizio, a meno che la richiesta di accesso sia eccessiva o gli sia già stato dato seguito nei 12 mesi precedenti, oppure la comunicazione delle informazioni causi un lavoro considerevole. I dettagli delle eccezioni alla gratuità del diritto di accesso sono disciplinate nel regolamento d'esecuzione.

Il contenuto dell'informazione non è più disciplinato unicamente nel regolamento d'esecuzione (art. 18 cpv. 2), ma viene ripreso e precisato direttamente nella legge nell'articolo 27 capoverso 2. All'articolo 27 capoverso 3 si precisa che la consultazione diretta dei propri dati può avvenire presso il titolare dell'elaborazione e/o, se del caso, presso il responsabile dell'elaborazione. Per il resto, la norma rimane invariata rispetto all'attuale articolo 23 capoverso 3.

Articolo 28
L'articolo 28 concernente le limitazioni al diritto di accesso non subisce variazioni rispetto all'attuale articolo 24 LPDP. Esso prevede, al capoverso 1, che il diritto di accesso ai propri dati personali possa essere limitato in presenza di interessi pubblici o privati preponderanti contrari. Gli interessi pubblici possono essere previsti dalla legge e essere dati in caso di sicurezza, oppure quando è pendente una procedura giudiziaria. Se sono presenti interessi privati preponderanti contrari di terze persone, il loro nome e i loro dati non devono essere accessibili al richiedente l'accesso, in particolare se esistono indizi di possibili rischi di violazioni illecite della loro personalità o di altri loro interessi giuridicamente protetti. Se l'inaccessibilità ai dati di terzi non è possibile, va effettuata una nuova ponderazione degli interessi, rispettivamente vanno oscurate perlomeno parte delle informazioni riguardanti i terzi.

Il capoverso 2 è inteso tutelare la persona interessata dal confronto con dati personali che la riguardano e che sono particolarmente delicati, segnatamente nel settore della salute, la cui trasmissione alla persona interessata può essere affidata a una persona di fiducia, vicina all'interessato.

Al capoverso 3 sono previste delle fattispecie che possono giustificare la limitazione o il rifiuto dell'accesso, a meno che l'istante sia in grado di dimostrare un interesse meritevole

di tutela. Si tratta dei casi in cui la richiesta di accesso comporta un onere di risorse umane, organizzative o temporali eccessive, per le quali il richiedente non intende sopportarne le spese, oppure quando i dati sono già definitivamente archiviati, e quindi più difficilmente recuperabili rispetto a dati ancora produttivi gestiti presso il titolare dell'elaborazione, o sono elaborati senza riferimento a persone specifiche secondo l'articolo 22.

Articolo 29
Il diritto di rettifica (vedi art. 16 Direttiva (UE) 2016/680) non presuppone più la dimostrazione di un interesse meritevole di tutela da parte del richiedente. La rettifica deve avvenire, inoltre, senza oneri finanziari per il richiedente ed entro un termine ragionevole (cpv. 1). Se il titolare dell'elaborazione contesta l'inesattezza, gli incombe il fardello della prova dell'esattezza dei dati, se la prova dell'inesattezza non può essere pretesa dall'istante (cpv. 2).

Articolo 30
Per esercitare il diritto di blocco, non è necessario che la persona interessata faccia valere, renda verosimile o dimostri un interesse particolare. In altre parole, il diritto di blocco è incondizionato. In questo senso, l'autorità non dispone di un margine di apprezzamento: essa deve attuare il blocco non appena la persona interessata abbia espresso chiaramente la volontà di esercitarlo.

Secondo la lettera b), nonostante il blocco, la comunicazione di dati personali da parte di enti soggetti alla legge è possibile se il destinatario rende verosimile che la persona interessata rifiuta il proprio consenso o blocca la comunicazione per impedirgli l'attuazione di pretese giuridiche (statuite, ad esempio, in una decisione cresciuta in giudicato) o la difesa di altri interessi preponderanti degni di protezione. La presenza di tali estremi va valutata puntualmente, previa ponderazione di tutti gli elementi e gli interessi in gioco. Alla persona interessata deve essere data facoltà di esprimersi preventivamente, a meno che ciò sia impossibile o esiga mezzi sproporzionati. Se la trasmissione dei dati in attuazione di una decisione cresciuta in giudicato dovesse compromettere legittimi interessi della persona interessata, quest'ultima deve attuare i necessari passi al fine di ottenere la modifica della decisione in questione, e non avvalersi del diritto di blocco per impedire l'attuazione della stessa.
Il disposto sul diritto di blocco ha portata limitata ai casi in cui non è pendente una procedura giudiziaria o non si applica un ordinamento procedurale secondo l'articolo 4 capoverso 2 LPDP.

Il capoverso 3 prevede il principio secondo cui il blocco segue i dati, vale a dire che il destinatario legittimato a riceverli in virtù del capoverso 2 è però vincolato dal blocco nei confronti di terzi.

Articolo 31
Anche per il diritto di interruzione, si rinuncia a esigere dal richiedente la dimostrazione di un interesse meritevole di tutela, nel senso che egli non deve dimostrare l'utilità pratica che una tale interruzione avrebbe per lui (vedi art. 9 STE 108, art. 54 Direttiva (UE) 2016/680; DTF 131 II 649, consid. 3.1). Per quanto riguarda il fardello della prova dell'illiceità, c'è un rovesciamento del fardello della prova a carico del titolare del trattamento, poiché a portare tale prova risulta più facile al titolare del trattamento, ritenuto che di principio ogni sua elaborazione di dati è giustificata da una base legale. Inoltre,

viene aggiunto il diritto di esigere dal titolare dell'elaborazione che i dati elaborati in modo illecito non vengano comunicati a terzi. A parte alcuni adeguamenti terminologici, la norma non subisce per il resto altri cambiamenti rispetto all'attuale articolo 26 LPDP.

Articolo 32
L'odierno articolo 27 LPDP viene ripreso nel nuovo articolo 11 concernente l'obbligo d'informare in caso di rettifica, cancellazione o distruzione di dati personali. Per il resto, la norma non subisce cambiamenti.

Capitolo decimo
L'attuale articolo 30 LPDP sulla funzione e organizzazione dell'Incaricato cantonale della protezione dei dati viene scorporato in quattro norme distinte concernenti a) la nomina, l'attribuzione e la destituzione, b) lo statuto, c) le risorse e d) il segreto d'ufficio.

Articolo 33
Per migliorare la struttura e la chiarezza, la nomina e l'attribuzione amministrativa dell'Incaricato vengono disciplinate in tre nuovi capoversi (cpv. 1-3), senza subire cambiamenti sostanziali rispetto all'attuale articolo 30 capoverso 1. La norma prevede i motivi di rimozione dell'Incaricato, conformemente all'articolo 43 cifra 4 Direttiva (UE) 2016/680. L'Incaricato è per il resto inserito nel quadro di funzionario LORD.

Articolo 34
L'elaborazione di dati da parte di un'autorità è sottoposta alla vigilanza di un organo di controllo indipendente, come prescritto dal diritto internazionale applicabile anche alla Svizzera e a tutti i Cantoni. Essa va pertanto riconosciuta sotto il profilo istituzionale e funzionale (capoverso 1). La procedura di nomina dell'Incaricato – poiché riconducibile a meccanismi parlamentari – accentua la centralità dell'indipendenza. Al Consiglio di Stato spettano la nomina, il vaglio del rapporto di attività congiuntamente con il Gran Consiglio e l'attribuzione amministrativa del servizio dell'Incaricato (art. 30 cpv. 1 LPDP). L'indipendenza dell'Incaricato mira a creare una funzione neutrale e riconosciuta come effettivo e credibile garante dei diritti e delle libertà fondamentali in relazione all'elaborazione di dati personali. Poiché agisce a tutela di diritti e interessi di rilievo costituzionale, l'Incaricato deve essere esente da qualsiasi tipo d'influenza, anche indiretta, e ciò ancor più nel quadro del nuovo diritto internazionale in materia di protezione dei dati personali, attualmente recepito nel diritto federale e cantonale.

Il capoverso 2 recepisce il diritto superiore (art. 42 cifra 3 Direttiva (UE) 2016/680), secondo cui i membri delle autorità di controllo si astengono da qualsiasi azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.

Il capoverso 3 precisa che l'adempimento dei compiti dell'Incaricato deve essere, di regola, esente da costi per la persona interessata (art. 46 cifra 3 Direttiva (UE) 2016/680). In caso di richieste d'intervento palesemente ingiustificate, infondate o eccessive (in particolare, in caso di eccessiva ripetizione della richiesta), l'Incaricato può chiedere un'equa partecipazione ai costi, sulla base del tariffario usuale per i costi amministrativi, oppure può rifiutare l'intervento. In tal caso, l'onere della prova dell'infondatezza o eccessività della richiesta è portato dall'Incaricato.

Articolo 35
Il capoverso 1 ricorda che le risorse attribuite all'Incaricato devono essere adeguate, vale a dire quantitativamente proporzionate alle effettive e concrete esigenze del servizio della protezione dei dati, e disporre di elevate competenze professionali per poter far fronte in modo efficiente ed efficace alle complesse mansioni che si pongono (art. 42 cfr. 4 Direttiva (UE) 2016/680, art. 16 cfr. 6 STE 108). Si deve in particolare tenere conto del fatto che l'Incaricato è obbligato a accertare i fatti d'ufficio per tutte le richieste di un suo intervento (art. 38 cpv. 1).

Secondo l'articolo 42 cfr. 5 Direttiva (UE) 2016/680, l'autorità di controllo seleziona il proprio personale. Nella presente revisione, si precisa che si tratta di un coinvolgimento nella selezione (capoverso 2). Le competenze governative in materia di nomina rimangono invariate.

Oltre alle risorse umane, tecniche e infrastrutturali necessarie, il diritto superiore prevede che l'Incaricato sia dotato di risorse finanziarie adeguate (art. 42 cfr. 4 Direttiva (UE) 2016/680) e di cui dispone liberamente una volta approvate dal Gran Consiglio (capoversi 3 e 4).

Articolo 36
Nell'esercizio delle sue funzioni, l'Incaricato e il personale addetto alla protezione dei dati soggiacciono al segreto d'ufficio generale previsto dall'ordinamento del personale pubblico (art. 29 della legge sull'ordinamento degli impiegati dello Stato e dei docenti; LORD; RL 173.100). Nel caso in cui venga svolta un'inchiesta su una determinata elaborazione di dati il cui titolare è soggetto a un segreto d'ufficio qualificato, l'Incaricato e il suo personale vi soggiacciono ugualmente.

Articolo 37
L'articolo 37 elenca i compiti attribuiti all'Incaricato:
a. L'attuale articolo 30a lettera a) subisce una modifica unicamente per quanto riguarda il richiamo delle norme legali ivi previste. Per il resto, rimane invariato.
b. L'articolo 37 lettera a) viene affiancato da una seconda norma, l'articolo 37 lettera b), sulla sorveglianza dello Stato, quando quest'ultimo non agisce in virtù di un potere sovrano, ma come soggetto di diritto privato in un rapporto paritario con un altro soggetto giuridico. Non diventando un privato, ma agendo unicamente come tale, lo Stato rimane assoggettato alla vigilanza dell'Incaricato cantonale della protezione dei dati secondo le norme sulla vigilanza previste dalla presente legge, non dell'Incaricato federale della protezione dei dati e della trasparenza. Tuttavia, le norme materiali di protezione dei dati applicabili sono quelle previste dalla LPD federale per la protezione dei dati da parte di privati (art. 3 cpv. 2).
c. La lettera c) riprende e precisa l'attuale articolo 30a lett. b), e prevede che tra i compiti dell'Incaricato figuri la sensibilizzazione degli organi pubblici responsabili sulla protezione dei dati e sugli obblighi e responsabilità che ne derivano, nonché il pubblico sull'istituzione e sulle facoltà dell'Incaricato, sui diritti e sulle responsabilità dei cittadini in materia di auto-tutela informazionale. Si tratta di attività di informazione, di formazione e di consiglio, anche tramite eventi informativi e corsi di perfezionamento.
d. La norma riprende l'attuale articolo 30a lettera d) e subisce una leggera riformulazione. Per il resto, rimane invariata. L'Incaricato è la figura di riferimento per gli organi pubblici

in materia di protezione dei dati. Copre anche la funzione di organo consultivo del Cantone, oggi prevista dall'articolo 30a lettera i) LPDP.

e. La norma riprende l'attuale articolo 30a lettera c). Per il resto, rimane invariata nel contenuto. L'Incaricato è inteso essere una figura di ausilio sia per le autorità sia per le persone interessate nel caso in cui si pongano questioni di protezione dei dati tra di esse.
f. Questa norma riprende l'attuale articolo 30a lettera e) senza variazioni materiali. L'Incaricato è autorità propositiva di soluzioni nel caso di violazioni o di rischi di violazione della protezione dei dati. Questa funzione può, se del caso, portare all'emissione di una raccomandazione secondo il nuovo articolo 38 LPDP.
g. Riprende l'attuale articolo 30a lettera f), senza modifiche materiali. L'Incaricato è l'organo responsabile della valutazione di progetti legislativi rilevanti per la protezione dei dati.
h. Riprende l'attuale articolo 30a lettera g). L'Incaricato vigila e, se del caso, interviene, presso gli incaricati comunali della protezione dei dati.
i. Riprende l'attuale lettera h), senza modifiche materiali.
j. Riprende l'attuale lettera i), senza modifiche materiali.
k. Ai compiti dell'Incaricato viene aggiunto quello della formazione continua sua e del personale addetto alla protezione dei dati, in particolare in materia di tecnologie dell'informazione e della comunicazione, nella misura in cui hanno un'incidenza sulla protezione dei dati. La formazione continua implica un budget adeguato (vedi art. 35 cpv. 3 e 4).

Articolo 38

Secondo il diritto internazionale superiore, la funzione di autorità di controllo in materia di protezione dei dati implica dei poteri d'investigazione e d'intervento effettivi (inchiesta), al fine di poter svolgere i rispettivi compiti legali in modo compiuto, efficace e credibile (art. 47 Direttiva (UE) 2016/680, art. 15 cfr. 2 lettera a Convenzione STE 108). Nell'esercizio delle sue funzioni e dei suoi poteri, l'Incaricato applica il diritto sulla procedura amministrativa. Può agire di propria iniziativa, allorquando nell'esercizio delle sue funzioni constata una possibile criticità legata alla protezione dei dati, oppure su segnalazione di terze persone o autorità (capoverso 1). In quest'ultimo caso, l'Incaricato deve trattare la segnalazione come una denuncia di diritto amministrativo (non penale) all'autorità di vigilanza ed accertare i fatti d'ufficio. L'Incaricato può rinunciare a aprire un'inchiesta se la violazione della protezione dei dati è di poca importanza. Può rinunciare all'inchiesta anche se appare sufficiente una consulenza al titolare dell'elaborazione, poiché la problematica di protezione dei dati è minore. La persona o l'organo segnalante può ricorrere davanti alla Commissione della protezione dei dati contro la decisione dell'Incaricato di non entrata in materia o di mancata informazione secondo il capoverso 2 (art. 52 e 53 Direttiva (UE) 2016/680, art. 15 cfr. 4 Convenzione STE 108). Viene quindi istituito un diritto alla denuncia della persona interessata e un dovere dell'Incaricato di trattarla d'ufficio.

Nel capoverso 2 si introduce l'obbligo dell'Incaricato di informare la persona o l'organo segnalante sullo stato e sulle conclusioni dell'inchiesta entro congruo termine, di principio entro tre mesi (art. 52 Direttiva (UE) 2016/680, art. 15 cfr. 4 Convenzione STE 108). Il segnalante non diventa parte dell'inchiesta, e quindi non ne acquisisce i diritti, a meno che il segnalante sia una persona fisica personalmente interessata dall'elaborazione di dati in questione. In tal caso, va garantito tra l'altro il diritto di essere sentito.

L'ampio potere d'investigazione dell'Incaricato implica l'obbligo del titolare dell'elaborazione di fornire tutte le informazioni sull'elaborazione di dati necessarie allo svolgimento della sua missione di vigilanza, di garantire la consultazione di tutti i documenti, le visite e le dimostrazioni dell'elaborazione di dati all'Incaricato (vedi art. 47 cfr. 1 Direttiva (UE) 2016/680). Gli organi interessati non possono opporre all'Incaricato nessuna norma di confidenzialità (segreto d'ufficio o segreto d'ufficio qualificato). Per l'ottenimento di documenti e informazioni, l'Incaricato può imporre un termine (capoverso 3).

La facoltà di emettere delle raccomandazioni permane (vedi attuale art. 30b cpv. 4 LPDP), con la precisazione che la raccomandazione può prevedere anche la sospensione di un'elaborazione di dati, fino a ripristino delle condizioni legali, tecniche e/o organizzative del caso (capoverso 4). L'autorità superiore del titolare dell'elaborazione è informata della raccomandazione.

Il capoverso 5, che riprende l'attuale articolo 30b capoverso 5 LPDP, prevede la facoltà dell'Incaricato di emettere una raccomandazione con effetto immediato nel caso in cui interessi meritevoli di protezione di una persona sono in modo evidente minacciati o lesi. Se la sospensione immediata di un'elaborazione dovesse compromettere seriamente l'esecuzione di compiti legali, è ipotizzabile una procedura super-cautelare e sommaria davanti alla Commissione cantonale per la protezione dei dati e la trasparenza, con tempistiche molto ridotte (10-15 giorni dal momento dell'emanazione della raccomandazione fino alla decisione della Commissione), introdotta dal titolare dell'elaborazione o dall'autorità superiore competente. L'Incaricato, l'organo interessato o l'autorità superiore competente possono ricorrere contro la decisione della Commissione presso il Tribunale amministrativo cantonale.

Nel capoverso 6 si introduce l'obbligo del titolare dell'elaborazione o dell'autorità superiore competente di dichiarare entro congruo termine, di norma entro un mese, se intendono seguire, in tutto o in parte, la raccomandazione.

Parallelamente alla facoltà, già prevista dal diritto positivo (art. 31b cpv. 6 LPDP), di portare la propria raccomandazione davanti all'autorità superiore competente (la quale, con il nuovo diritto, sarà la Commissione cantonale della protezione dei dati e la trasparenza) nel caso in cui il responsabile la rigetti o non gli dia seguito (cpv. 10), nel capoverso 7 viene introdotta la facoltà dell'Incaricato di prendere una decisione con la quale obbliga l'autorità ad applicare tutte o parte delle misure contenute nella raccomandazione, rispettivamente di decidere immediatamente, senza emissione di una raccomandazione, nel caso in cui sia verosimile che il responsabile dell'elaborazione rigetti la raccomandazione o non gli dia seguito.

Il capoverso 8 stabilisce la via ricorsuale contro la decisione dell'Incaricato secondo il capoverso 7.

Il capoverso 9 stabilisce la via ricorsuale contro la decisione della Commissione secondo il capoverso 8.

Nel caso in cui, invece, l'Incaricato non dovesse prendere una propria decisione secondo il capoverso 7, egli può portare la raccomandazione respinta o non seguita davanti alla Commissione cantonale per la protezione dei dati e la trasparenza (capoverso 10).

Articolo 39
La norma sulla funzione e composizione della Commissione cantonale per la protezione dei dati e la trasparenza rimane invariata. Viene tolto il vincolo secondo il quale il presidente deve essere un magistrato o un ex magistrato.

Articolo 40
Parimenti, la norma sulla competenza e procedura della Commissione rimane invariata, fatto salvo il capoverso 4, che non prevede più l'Incaricato come organo di conciliazione. Nell'esercizio delle sue funzioni, l'Incaricato può essere chiamato a prendere posizione o emettere pareri sulla conformità di una determinata elaborazione di dati con la LPDP. Poiché una pratica precedentemente elaborata dall'Incaricato può essere portata davanti alla Commissione da parte della persona interessata, il tentativo di conciliazione andrebbe promosso presso la commissione stessa (art. 23 legge sulla procedura amministrativa; RL 165.100; LPAmm), oppure presso un altro organo indipendente di mediazione che non si sia già precedentemente espresso sulla questione.

Articolo 41
La norma riprende l'attuale articolo 31b LPDP, precisando che si tratta di un responsabile della protezione dei dati, e non di un'autorità di vigilanza vera e propria.

Articolo 42
La norma riprende l'attuale articolo 32 LPDP, senza modifiche materiali.
L'articolo 33 della legge vigente, che commina la sanzione nel caso di violazione del segreto d'ufficio, è abrogato poiché corrisponde materialmente all'articolo 320 CP.

Articolo 43
La norma riprende l'attuale articolo 37 LPDP sulle norme materiali d'esecuzione, completandola con ulteriori oggetti previsti dal presente disegno di legge che necessitano di un disciplinamento materiale.

Articolo 44
Trattandosi di una revisione totale, la legge sulla protezione dei dati personali del 9 marzo 1987 è abrogata.

Articolo 45
Diversi atti normativi rinviano alla legge del 1987 attualmente in vigore; con l'entrata in vigore della nuova legge è necessario adeguare tali rimandi.

Articolo 46
Il Consiglio di Stato fisserà la data di entrata in vigore della legge in modo da garantire un'informazione adeguata.

Modifica di altri atti normativi

Legge di applicazione della legge federale sull'armonizzazione dei registri e concernente il controllo degli abitanti e la banca dati movimento della popolazione del 5 giugno 2000

Per motivi di adeguatezza della sede delle norme sulla trasmissione dei dati del controllo abitanti comunale e cantonale, la legge di applicazione della legge federale sull'armonizzazione dei registri e concernente la banca dati movimento della popolazione del 5 giugno 2000, riprenderà gli attuali articoli 12 e 13 LPDP, che non verranno quindi ripresi nella nuova legge sulla protezione della persona in relazione all'elaborazione di dati personali.

L'articolo 10a capoverso 2 viene precisata rispetto all'attuale formulazione, sostituendo il termine di trasmissione in ordine sistematico con il più preciso termine di trasmissione sotto forma di lista. Inoltre, il rinvio all'attuale articolo 4 capoverso 7 concernente i dati neutri (cognome, nome, indirizzo) è sostituito con l'elenco di tali dati, perché la norma sui dati neutri non viene più ripresa. Infine, viene precisato che, oltre al nome, cognome e indirizzo, la trasmissione implica il o i dati concernenti una o più caratteristiche comuni delle persone interessate (ad esempio, l'anno di nascita), richieste dall'istante.

Nell'articolo 10b viene precisato che il Servizio cantonale del movimento della popolazione può trasmettere dati unicamente alle condizioni e modalità previste dall'articolo 10a capoverso 2, vale a dire il cognome, il nome e l'indirizzo di persone aventi una o più caratteristiche comuni, esclusivamente per scopi ideali. L'esistenza o meno di uno scopo ideale viene valutata attentamente in ogni singolo caso concreto. È dato lo scopo ideale, ad esempio, quando si persegue un interesse, un ideale o un'utilità pubblica, segnatamente la promozione della cultura, della salute pubblica e/o dell'educazione alla socializzazione dei giovani, (è il caso, ad esempio, delle società sportive), oppure del sostegno agli anziani o a persone bisognose di aiuto. In simili casi, la riscossione di un'eventuale tassa d'iscrizione alla rispettiva società o organizzazione va intesa unicamente come copertura dei costi gestionali e amministrativi, e non come scopo lucrativo.
Per contro, le trasmissioni nei singoli casi secondo l'articolo 10a capoversi 1 e 3 del progetto rimangono di competenza esclusiva dei Comuni. Per il resto, la norma richiama la facoltà di trasmettere dati personali senza riferimento a persone specifiche, segnatamente per scopi statistici, pianificatori, scientifici e di ricerca secondo l'articolo 22 del progetto nonché, più in generale, la trasmissione di dati in virtù di specifiche norme di assistenza amministrativa previste dal diritto settoriale.
Infine, viene eliminato il riferimento al servizio che gestisce il Registro degli stranieri, poiché tale servizio non è più competente per le trasmissioni di dati sul movimento della popolazione straniera ai sensi della legislazione sull'armonizzazione dei registri.

Nell'articolo 10c viene ripreso l'attuale articolo 14 capoverso 1 LPDP (nuovo art. 21 cpv. 1), secondo cui la trasmissione è comunque sempre vincolata dalla ponderazione degli interessi in gioco.

V. ORGANIZZAZIONE DELLA PROTEZIONE DEI DATI

All'Incaricato sono garantite le risorse umane adeguate per poter fare fronte ai compiti assegnatigli dalla legislazione sulla protezione dei dati.

Tra i nuovi compiti, diretti e indiretti, dell'Incaricato che nasceranno con l'entrata in vigore della presente revisione vi saranno, in particolare:
- l'accertamento d'ufficio di ogni segnalazione (nuovo 38 cpv. 2 LPDP);
- le valutazioni delle notifiche della violazione della protezione dei dati (nuovo art. 16 LPDP);
- la creazione di nuove direttive, modelli e schede informative (segnatamente negli ambiti della prova del rispetto delle disposizioni della protezione dei dati da parte del titolare [nuovo art. 8 LPDP], dell'obbligo d'informare in occasione della raccolta di dati personali [nuovo art. 10 LPDP], della valutazione d'impatto [nuovo art. 13 LPDP], del registro del titolare [nuovo art. 26 LPDP], della protezione dati sin dalla progettazione [nuovo art. 14 LPDP], dei diritti [nuovi art. 27 e seguenti LPDP]).

VI. RELAZIONE CON IL PIANO DI LEGISLATURA E CONSEGUENZE FINANZIARIE

1. Piano di legislatura

Il progetto di revisione totale della legislazione cantonale in materia di protezione dei dati non figura nel programma di legislatura 2019-2023 adottato dal Consiglio di Stato nel gennaio 2020. L'adozione della riforma è conseguenza del diritto federale e degli impegni internazionali sottoscritti dalla Confederazione.

2. Conseguenze finanziarie

Attualmente all'ufficio sono attribuite due unità (incaricato cantonale e giurista); esso si avvale del segretariato dei Servizi giuridici del Consiglio di Stato. Il Consiglio di Stato intende potenziare l'ufficio dell'Incaricato cantonale della protezione dei dati con una ulteriore unità di giurista. Trattandosi di un nuovo onere (escluso dalla tendenza), l'aumento dell'organico è da effettuare mediante l'attribuzione di una ulteriore unità PPA (Piano dei posti autorizzati) all'ufficio dell'Incaricato che dovrà essere dedotta dalla dotazione di compiti futuri. Con il potenziamento proposto si rafforzerebbe in primo luogo l'ambito giuridico. A dipendenza delle esigenze, una parte del potenziamento potrebbe essere attribuita a una persona che si occupi degli aspetti informatici mediante la commutazione in una funzione equivalente di collaboratore scientifico. I costi a carico dello Stato legati all'attribuzione di un'unità di giurista (o collaboratore scientifico) ammontano a circa 150'000 franchi l'anno.

I compiti dell'Incaricato sono stabiliti negli articoli 37 e 38 del progetto e sono descritti nel commento a queste due norme. Come abbiamo indicato nel capitolo V i nuovi compiti comprendono l'accertamento d'ufficio di ogni segnalazione, l'esame sulle notifiche ricevute in merito a violazioni della protezione dei dati, l'elaborazione di direttive e altra documentazione. L'ufficio dell'Incaricato dovrà rafforzare la sua attività di vigilanza e di ispezioni sulle banche dati del Cantone, dei Comuni e degli altri organi pubblici o preposti a compiti pubblici. Si tratta di un compito che non si riesce a svolgere con le risorse attuali,

seppur già rientri nelle incombenze dell'Incaricato. In seguito all'entrata in vigore del diritto superiore, le facoltà dell'Incaricato in materia di emanazione di decisioni e di raccomandazioni vengono estese ed è dato un maggiore rilievo alla formazione e alla sensibilizzazione degli organi pubblici responsabili e del pubblico.

VII. CONSEGUENZE A LIVELLO DI ENTI LOCALI E ALTRE ISTITUZIONI

Il rafforzamento della protezione dei dati previsto dal presente progetto di nuova legge cantonale sulla protezione delle persone in relazione all'elaborazione di dati personali si riflette su tutti i soggetti alla legge, quindi anche sui comuni e sugli altri enti locali e alle istituzioni parastatali o private cui sono delegati compiti di diritto pubblico. Oltre all'obbligo di legiferare in materia di elaborazioni sistematiche di dati – già presente nella legge dal 1° gennaio 2016 – i soggetti alla legge sono chiamati in particolare a tenere conto e attuare il rafforzamento dei diritti dei cittadini e a rispettare i corollari obblighi del titolare dell'elaborazione di dati. Si tratta in particolare degli obblighi di informazione in occasione della raccolta, rettifica, cancellazione o distruzione di dati personali (art. 10 e seguenti), dell'obbligo della valutazione d'impatto di elaborazioni di dati sui diritti della personalità dell'individuo (art. 13), della protezione dei dati fin dalla progettazione (art. 14), della consultazione preventiva dell'Incaricato cantonale in determinate circostanze e della notifica della violazione della protezione dei dati (art. 15 e 16).

VIII. COMPATIBILITÀ CON IL DIRITTO FEDERALE E CON IL DIRITTO CANTONALE

Il recepimento del diritto internazionale superiore sulla protezione dei dati avviene in conformità con la ripartizione costituzionale delle competenze legislative tra Confederazione e Cantoni e costituisce un rafforzamento dei diritti e delle libertà fondamentali già previste dalle Costituzioni cantonali e federali e attuate negli ordinamenti giuridici federali e cantonali.

IX. RELAZIONI CON IL DIRITTO EUROPEO

Il progetto di revisione totale della legge cantonale sulla protezione dei dati attua la trasposizione della Direttiva (UE) 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Recepisce altresì il Protocollo di emendamento alla Convenzione STE 108 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale e il suo Protocollo aggiuntivo STE 181 concernente le autorità di controllo e i flussi internazionali di dati. Infine, si adegua al Regolamento (UE) 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR) e alle raccomandazioni della Commissione europea nei confronti della Svizzera. La trasposizione del diritto internazionale superiore avviene conformemente alle raccomandazioni della Conferenza dei Governi cantonali del 2 febbraio 2017.

X. CONCLUSIONE

In conclusione, il Consiglio di Stato invita il Gran Consiglio ad accogliere il disegno di legge annesso al messaggio.

Vogliate gradire, signora Presidente, signore e signori deputati, l'espressione della massima stima.

Per il Consiglio di Stato

Il Presidente: Raffaele De Rosa
Il Cancelliere: Arnoldo Coduri

Disegno di

Legge
sulla protezione dei dati personali
(LPDP)
del .....

IL GRAN CONSIGLIO
DELLA REPUBBLICA E CANTONE TICINO

visto l'articolo 8 capoverso 2 lettera d della Costituzione della Repubblica e Cantone Ticino;
visto il messaggio del Consiglio di Stato n. 8281 del 17 maggio 2023,

decreta:

Capitolo primo
Scopo, campo d'applicazione e definizioni

Scopo
Art. 1
La presente legge ha lo scopo di proteggere i diritti fondamentali, in particolare la personalità e la sfera privata, delle persone i cui dati personali sono elaborati dai soggetti di all'articolo 3 della presente legge.

Campo d'applicazione
a) materiale
Art. 2
La legge si applica ad ogni elaborazione di dati personali, indipendentemente dagli scopi, dalle procedure e dalle modalità utilizzate.

b) istituzionale e personale
Art. 3
[1]Alla legge sottostanno il Cantone, i Comuni, le altre corporazioni e istituti di diritto pubblico e i loro organi. A questi sono parificate le persone fisiche e giuridiche di diritto privato, cui siano delegati compiti di diritto pubblico.
[2]La legge non si applica nella misura in cui uno di questi enti partecipa a una attività economica che non deriva da un potere sovrano. Rimangono riservate le competenze di vigilanza dell'Incaricato cantonale della protezione dei dati ai sensi dell'articolo 37 lettera b e dell'articolo 38.

c) procedurale
Art. 4
[1]La protezione dei dati nelle procedure amministrative di prima istanza è retta dalle disposizioni della presente legge.
[2]La protezione dei dati nelle procedure giudiziarie e in quelle secondo gli ordinamenti procedurali sono retti dal relativo diritto procedurale applicabile. La presente legge è tuttavia applicabile, ad eccezione delle norme sulla vigilanza, laddove il diritto procedurale non disciplina la protezione dei dati in modo equivalente alla presente legge.

Definizioni
Art. 5

[1]Sono dati personali le indicazioni o informazioni che direttamente o indirettamente permettono di identificare una persona, sia essa fisica o giuridica.
[2]Sono dati personali meritevoli di particolare protezione le informazioni o indicazioni concernenti:
a) le opinioni o le attività religiose, filosofiche, politiche o sindacali;
b) l'appartenenza a una razza o a un'etnia;
c) lo stato fisico, mentale o psichico;
d) la sfera intima;
e) i dati genetici;
f) i dati biometrici;
g) i dati concernenti procedure, perseguimenti e sanzioni di natura amministrativa, penale e civile;
h) i dati concernenti le misure di assistenza sociale.
[3]È considerata elaborazione di dati personali ogni operazione intesa, segnatamente, a raccogliere, registrare, utilizzare, modificare, trasmettere, bloccare, conservare, cancellare o distruggere questi dati.
[4]È considerata elaborazione nel singolo caso l'elaborazione di dati puntuale.
[5]È considerata elaborazione sistematica l'operazione che implica regolarità o durata.
[6]È procedura di richiamo il modo di consultazione automatizzato o diretto dei dati, tramite il quale l'autorità che richiede i dati decide di propria iniziativa il momento, il modo e l'estensione dell'accesso nel caso specifico, e ciò senza controllo preventivo dell'autorità che detiene i dati, ossia senza che questa esamini la liceità della consultazione e la sua motivazione ad ogni singolo accesso.
[7]È considerato interfacciamento o associazione di banche dati il loro collegamento per sincronizzare i dati tra il fornitore di dati e l'utente dei dati.
[8]È considerata banca dati o archivio di dati qualsiasi insieme di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia strutturato, centralizzato, decentralizzato o ripartito in modo funzionale o geografico.
[9]È considerata profilazione l'elaborazione di dati comprendente la valutazione di determinate caratteristiche di una persona sulla base di dati personali elaborati automaticamente, in particolare per analizzare o predire il rendimento professionale, la situazione economica, la salute, il comportamento, gli interessi o le preferenze, il luogo di soggiorno o gli spostamenti.
[10]È titolare dell'elaborazione di dati colui che, singolarmente o insieme ad altri, determina l'elaborazione dei dati, in particolare le finalità, il contenuto, la trasmissione, le modalità e la procedura.
[11]È mandatario dell'elaborazione di dati colui che elabora dati personali su mandato del titolare dell'elaborazione.
[12]È partecipante di una banca dati chi ha diritto di immettervi dati e di consultarli tramite procedura di richiamo, senza disporre delle facoltà del titolare della banca dati.
[13]È utente di una banca dati chi ha diritto di consultare i dati tramite procedura di richiamo.
[14]È destinatario di dati chi, regolarmente o puntualmente, riceve dati personali.
[15]Per consenso ai sensi della presente legge s'intende la manifestazione di volontà della persona interessata avvenuta in modo libero, specifico, informato, inequivocabile, verificabile e revocabile. Il consenso non può essere tacito.

Capitolo secondo

Motivi giustificativi e principi dell'elaborazione di dati personali

Motivi giustificativi
Art. 6
[1]I dati possono essere elaborati in modo sistematico se esiste una base legale. Se i dati sono meritevoli di particolare protezione, la base legale deve essere di rango formale.
[2]La base legale deve prevedere, in particolare, l'oggetto e lo scopo dell'elaborazione, la cerchia delle persone interessate, il titolare e il responsabile dell'elaborazione, gli organi partecipanti e gli utenti, i destinatari di dati, le modalità e le condizioni, la durata di conservazione dei dati e le misure di sicurezza.
[3]L'elaborazione di dati personali nel singolo caso può essere giustificata anche dalla necessità per l'adempimento di un compito legale o dal consenso della persona interessata.

Principi
Art. 7
[1]I dati personali possono essere elaborati soltanto in modo lecito.
[2]L'elaborazione dei dati deve essere conforme al principio della buona fede.
[3]I dati personali e il modo della loro elaborazione devono essere idonei e necessari all'adempimento del compito e deve sussistere un rapporto ragionevole tra lo scopo dell'elaborazione e la violazione della personalità che ne deriva.
[4]I dati personali non possono essere utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente erano stati raccolti.
[5]I dati personali devono possibilmente essere raccolti presso la persona interessata.
[6]I dati personali devono essere esatti e, nella misura in cui lo scopo dell'elaborazione lo richieda, completi.
[7]Chi elabora dati personali deve prendere misure appropriate di sicurezza per garantire la confidenzialità, l'integrità e la disponibilità dei dati. Prende, in particolare le misure appropriate contro la perdita, il furto e l'elaborazione illecita, in particolare la consultazione e la modifica illecita.

Capitolo terzo
Responsabilità e obblighi del titolare dell'elaborazione

Responsabilità
Art. 8
[1]Il titolare e, se del caso, il mandatario dell'elaborazione, gli organi partecipanti, gli utenti e i destinatari di dati sono responsabili della protezione dei dati nei rispettivi ambiti di competenza. In particolare, devono poter provare in ogni momento che rispettano le disposizioni relative alla protezione dei dati.
[2]La responsabilità civile per i danni causati a terze persone con l'elaborazione dei dati è retta dalla legge sulla responsabilità civile degli enti pubblici e degli agenti pubblici del 24 ottobre 1988.

Rettifica, cancellazione o distruzione di dati inesatti
Art. 9

Il titolare dell'elaborazione prende tutte le misure necessarie per rettificare, cancellare o distruggere d'ufficio i dati inesatti o incompleti rispetto alle finalità per le quali sono stati raccolti o elaborati.

Obbligo di informare in occasione della raccolta di dati personali
Art. 10
Il titolare dell'elaborazione informa la persona interessata su ogni raccolta di dati personali. Egli comunica alla persona interessata le informazioni necessarie affinché questa possa far valere i propri diritti e sia garantita la trasparenza dell'elaborazione, in particolare:
a) l'identità e le coordinate di contatto del titolare del trattamento;
b) lo scopo dell'elaborazione e la base legale;
c) il cambiamento dello scopo dell'elaborazione;
d) i dati o le categorie di dati elaborati;
e) se del caso, i destinatari o le categorie di destinatari cui sono comunicati dati personali;
f) i diritti della persona interessata;
g) se richieste, tutte le altre informazioni complementari necessarie a garantire un'elaborazione corretta e trasparente dei dati personali.

Obbligo di informare in occasione della rettifica, cancellazione o distruzione di dati personali
Art. 11
Il titolare dell'elaborazione informa i destinatari di dati di ogni rettifica, cancellazione o distruzione di dati, o di limitazioni alla loro elaborazione, avvenute d'ufficio o su richiesta della persona interessata, salvo se tale informazione si rivela impossibile o esige sforzi sproporzionati.

Eccezioni all'obbligo di informare
Art. 12
L'obbligo di informare di cui agli articoli 10 e 11 decade se una delle condizioni seguenti è adempiuta:
a) la persona interessata dispone già delle pertinenti informazioni;
b) l'elaborazione dei dati personali è prevista dalla legge;
c) l'informazione non è possibile o esige mezzi sproporzionati;
d) se interessi preponderanti di un terzo lo esigono;
e) se l'informazione pregiudica lo scopo del trattamento.

Valutazione d'impatto
Art. 13
Il titolare dell'elaborazione realizza una valutazione d'impatto relativa alla protezione dei dati quando v'è un rischio elevato di violazione della protezione dei dati. La valutazione d'impatto contiene almeno:
a) una descrizione generale delle procedure di elaborazione previste;
b) una valutazione dei rischi per la personalità e le libertà fondamentali delle persone interessate;
c) una presentazione e valutazione delle misure che intende implementare, segnatamente le garanzie e le misure di sicurezza tese a limitare tali rischi.

Protezione dei dati fin dalla progettazione
Art. 14

[1]Il titolare dell'elaborazione è tenuto ad adottare, sin dalla progettazione della stessa, i provvedimenti tecnici e organizzativi necessari affinché il trattamento sia conforme alle disposizioni sulla protezione dei dati, in particolare ai principi di cui all'articolo 7.
[2]I provvedimenti tecnici e organizzativi devono essere adeguati in particolare allo stato della tecnica, alla natura e all'estensione del trattamento dei dati, come pure al rischio che il trattamento comporta per la personalità e le libertà fondamentali delle persone interessate.

Consultazione preventiva e preavviso
Art. 15
[1]Il titolare dell'elaborazione sottopone tempestivamente per preavviso all'Incaricato cantonale della protezione dei dati i progetti seguenti:
a) progetti legislativi che prevedono l'elaborazione di dati personali;
b) progetti di elaborazione di dati i quali, per il tipo di elaborazione di dati o per la sensibilità dei dati elaborati, presentano un elevato rischio per i diritti della personalità e le libertà fondamentali delle persone interessate.
[2]Il regolamento d'esecuzione definisce una lista di progetti che devono essere sottoposti alla consultazione preventiva.
[3]Il preavviso non è vincolante.

Notifica della violazione della protezione dei dati
Art. 16
[1]Il titolare del trattamento notifica all'Incaricato, entro congruo termine, la violazione delle norme sulla protezione dei dati.
[2]La violazione della protezione dei dati è data quando la compromissione della sicurezza dei dati ha comportato la soppressione definitiva o la perdita di dati, la loro modifica o la loro divulgazione non intenzionale o illecita o la loro accessibilità da parte di terzi non autorizzati.
[3]Non sussiste l'obbligo di notifica di cui al capoverso 1 quando la violazione della protezione dei dati non presenta verosimilmente dei rischi per i diritti della personalità e le libertà fondamentali della persona interessata.
[4]Il titolare dell'elaborazione informa inoltre le persone interessate quando le circostanze lo esigono o l'Incaricato lo chiede. Si può rinunciare in tutto o in parte all'informazione, o la si può differire, se un interesse privato o pubblico preponderante lo esige.
[5]Il responsabile dell'elaborazione notifica tempestivamente ogni violazione della protezione dei dati al titolare dell'elaborazione.

Capitolo quarto
Trasmissione di dati personali

Trasmissione a organi pubblici
Art. 17
Possono essere trasmessi dati personali ad altri organi pubblici se:
a) l'organo responsabile vi è obbligato o autorizzato dalla legge speciale, oppure
b) i dati, nel caso specifico, sono indispensabili all'organo richiedente per l'adempimento dei suoi compiti legali, oppure
c) la persona interessata, nel caso specifico, ha dato il suo consenso o le circostanze permettono di presumerlo; trattandosi di dati personali meritevoli di particolare protezione, il consenso deve essere esplicito.

Trasmissione a persone private o al pubblico
a) a persone private
Art. 18
Dati personali possono essere trasmessi a persone private se:
a) il titolare dell'elaborazione vi è autorizzato o obbligato dalla legge speciale, oppure
b) la persona interessata ha reso i suoi dati accessibili pubblicamente e non si è formalmente opposta, ai sensi e nei limiti dell'articolo 29, alla loro trasmissione, oppure
c) la persona interessata, nel caso specifico, ha dato il suo consenso o le circostanze permettono di presumerlo; trattandosi di dati personali meritevoli di particolare protezione, il consenso deve essere esplicito.

b) al pubblico
Art. 19
Nell'ambito dell'informazione ufficiale del pubblico l'organo responsabile può trasmettere dati personali anche d'ufficio o in virtù della legge sull'informazione e la trasparenza dello Stato del 15 marzo 2011 (LIT) se:
a) i dati personali da trasmettere sono in rapporto con l'adempimento di compiti pubblici, e
b) sussiste un interesse pubblico preponderante alla pubblicazione dei dati.

Trasmissione di dati all'estero
Art. 20
[1]I dati personali non possono essere trasmessi all'estero qualora la personalità della persona interessata possa subirne grave pregiudizio, dovuto in particolare all'assenza di una legislazione che assicuri una protezione adeguata.
[2]Se manca una legislazione che assicuri una protezione adeguata, dati personali possono essere trasmessi all'estero soltanto se:
a) garanzie sufficienti, segnatamente contrattuali, assicurano una protezione adeguata all'estero;
b) nel caso specifico, la persona ha dato il suo consenso esplicito, libero e informato;
c) nel caso specifico, la trasmissione è indispensabile per tutelare un interesse pubblico preponderante oppure per accertare, esercitare o far valere un diritto in giustizia;
d) nel caso specifico, la trasmissione è necessaria per proteggere la vita o l'incolumità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole;
e) la persona interessata ha reso i dati accessibili a chiunque e non si è opposta formalmente alla loro elaborazione.
[3]Il titolare dell'elaborazione informa l'Incaricato cantonale della protezione dei dati sulle garanzie ai sensi del capoverso 2 lettera a.
[4]Laddove una protezione adeguata sia assicurata, la trasmissione è lecita se sono adempiute le condizioni valide per la trasmissione di dati in Svizzera.

Disposizioni comuni
Art. 21
[1]La trasmissione di dati personali può essere limitata o sottoposta a condizioni, in particolare alla sottoscrizione di una convenzione, qualora sia necessario per tutelare importanti interessi pubblici o privati o i dati si rivelino meritevoli di particolare protezione per la persona interessata.

[2]Dati personali oggetto di norme particolari di segretezza possono essere trasmessi solo alle condizioni previste esplicitamente dal diritto speciale.
[3]Il titolare dell'elaborazione può permettere l'accesso a dati personali mediante una procedura di richiamo o un interfacciamento di banche dati, qualora ciò sia previsto esplicitamente dal diritto. Dati personali meritevoli di particolare protezione possono essere resi accessibili mediante una procedura di richiamo o un interfacciamento di banche dati soltanto se lo prevede esplicitamente una legge in senso formale.
[4]Il titolare dell'elaborazione può rendere accessibili a chiunque dati personali mediante servizi di informazione e comunicazione automatizzati se una base legale prevede la pubblicazione di questi dati oppure se rende accessibili informazioni al pubblico in virtù della legge sull'informazione e la trasparenza dello Stato del 15 marzo 2011. Se non sussiste più l'interesse pubblico a renderli accessibili, questi dati devono essere tolti dal servizio di informazione e comunicazione automatizzato.

Capitolo quinto
Elaborazioni particolari

Elaborazioni senza riferimento a persone specifiche
Art. 22
[1]L'organo responsabile può elaborare o trasmettere a terzi dati personali per scopi impersonali, segnatamente statistici, pianificatori, scientifici e di ricerca, se:
a) i dati sono anonimizzati, non appena lo permette lo scopo dell'elaborazione;
b) il destinatario trasmette i dati soltanto con l'autorizzazione dell'organo responsabile;
c) i risultati dell'elaborazione sono pubblicati in una forma che non permetta d'identificare le persone interessate; e
d) il destinatario presenta le condizioni per il rispetto del segreto e delle altre disposizioni relative alla protezione e alla sicurezza dei dati.
[2]La trasmissione di dati a scopi impersonali è preceduta dalla conclusione di una convenzione sulla protezione dei dati.
[3]Dal momento che i dati personali sono anonimizzati in modo irreversibile, non si è più tenuti a osservare la presente legge.

Elaborazioni su mandato
Art. 23
[1]Il titolare dell'elaborazione può avvalersi di un mandatario per elaborare dati personali, se nessuna disposizione legale o contrattuale l'esclude.
[2]Se il titolare dell'elaborazione incarica un altro organo pubblico o terzi di elaborare dati personali, il mandatario è sottoposto al rispetto delle norme della presente legge alla stessa stregua del mandante. L'impegno a rispettare la presente legge deve essere garantito da condizioni, convenzioni o in altro modo.
[3]Senza esplicita autorizzazione derogante, il mandatario può utilizzare dati personali soltanto per il mandante e trasmetterli solo a quest'ultimo.

Capitolo sesto
Trattamento di dati nell'ambito di un progetto pilota

Progetto pilota
Art. 24

[1]Il Consiglio di Stato può autorizzare mediante decreto esecutivo il trattamento automatizzato di dati personali degni di particolare protezione nell'ambito di un progetto pilota quando un periodo di sperimentazione è necessario prima dell'elaborazione di una base legale in senso formale, in particolare per ragioni tecniche o organizzative.
[2]Prima di rilasciare un'autorizzazione il Consiglio di Stato raccoglie il parere dell'Incaricato.
[3]L'organo responsabile presenta un rapporto di valutazione al Consiglio di Stato. Il rapporto deve essere presentato entro due anni dall'avvio del trattamento e ne propone la continuazione o l'interruzione.
[4]Il trattamento decade al più tardi cinque anni dopo l'avvio se non è entrata in vigore una base legale in senso formale che lo autorizzi.

Capitolo settimo
Conservazione, archiviazione e distruzione dei dati

Scopo, modalità e termini di conservazione
Art. 25
[1]Il legislatore stabilisce, per ogni archivio di dati, i termini e le modalità di conservazione, archiviazione e distruzione dei dati, tenendo conto:
a) delle specifiche, obiettive e giustificate esigenze di utilizzazione e di prova per l'adempimento degli scopi per i quali sono stati lecitamente raccolti o elaborati;
b) di eventuali interessi degni di protezione delle persone interessate.
[2]Alla scadenza del termine legale di conservazione, il titolare dell'elaborazione offre all'istituto archivistico competente di riprendere tutti i documenti contenenti dati personali, conformemente alla legge sull'archiviazione e sugli archivi pubblici del 15 marzo 2011 (LArch).
[3]Il titolare dell'elaborazione distrugge i dati personali che l'istituto archivistico competente ha designato privi di valore archivistico, tranne quando tali dati sono resi anonimi e sono utilizzati per scopi statistici, di ricerca o per altri scopi impersonali.

Capitolo ottavo
Registri

Registro del titolare e registro centrale
Art. 26
[1]Il titolare dell'elaborazione tiene un registro dei suoi archivi di dati.
[2]L'incaricato cantonale della protezione dei dati gestisce il registro centrale degli archivi di dati.
[3]I registri sono pubblici e contengono, per ogni banca dati, indicazioni concernenti la denominazione, il titolare, lo scopo, i mezzi dell'elaborazione, la base legale, le categorie di dati personali elaborati, gli organi partecipanti e gli utenti.

Capitolo nono
Diritti della persona interessata

Diritto di accesso ai propri dati
a) principio
Art. 27
[1]Chiunque può esigere dal titolare dell'elaborazione informazioni in merito all'eventuale elaborazione di dati che lo riguardano.

[2]Il diritto di accesso non deve essere motivato.
[3]L'informazione contiene:
a) le indicazioni di cui all'articolo 10;
b) la durata di conservazione dei dati;
c) la provenienza dei dati.
[4]Le informazioni devono essere date:
a) in forma intellegibile;
b) entro un termine ragionevole;
c) di principio, gratuitamente;
d) su richiesta, per iscritto.
[5]A meno che importanti motivi lo impediscano, la persona interessata può, su richiesta, consultare i propri dati direttamente presso il titolare oppure, se del caso, presso il responsabile dell'elaborazione.

b) limitazioni
Art. 28
[1]L'informazione può essere limitata o rifiutata unicamente quando interessi pubblici o privati preponderanti lo esigono.
[2]Se l'informazione non può essere comunicata al richiedente perché ne avrebbe turbamento, essa può essere data a una persona di sua fiducia.
[3]Se l'istante non è in grado di dimostrare un interesse meritevole di tutela, l'informazione può inoltre essere limitata o rifiutata quando:
a) la stessa comporta un eccessivo onere amministrativo e l'istante non ne intende sopportare le spese;
b) i dati personali sono definitivamente archiviati;
c) i dati personali sono elaborati senza riferimento a persone specifiche.

Diritto di rettifica
Art. 29
[1]Chiunque può esigere dal titolare dell'elaborazione che dati personali inesatti siano rettificati gratuitamente e entro un termine ragionevole.
[2]Se il titolare dell'elaborazione contesta l'inesattezza, egli deve provare l'esattezza dei dati personali, se la prova dell'inesattezza non può essere pretesa dall'istante.
[3]Qualora non fosse possibile provare né l'esattezza né l'inesattezza di dati personali, in particolare se si tratta di dati che implicano una valutazione del comportamento umano, la persona interessata può richiedere che la propria versione sia anch'essa annotata.

Diritto di blocco
Art. 30
[1]La persona interessata può far bloccare in ogni momento la trasmissione dei suoi dati. Il diritto di blocco non deve essere motivato. L'organo responsabile può esigere che la domanda venga formulata per iscritto.
[2]Nonostante il blocco, la trasmissione è permessa se:
a) l'organo responsabile è obbligato a farlo dalla legge o da una decisione cresciuta in giudicato, oppure
b) il richiedente rende verosimile che la persona interessata ha fatto bloccare la trasmissione allo scopo di impedirgli l'attuazione di pretese giuridiche e la difesa di altri interessi degni di protezione. Alla persona interessata va data facoltà di esprimersi preventivamente, a meno che ciò sia impossibile o esiga mezzi sproporzionati.

[3]Nelle fattispecie di cui al capoverso 2, il destinatario legittimato a ricevere i dati è vincolato dal blocco degli stessi nei confronti di terzi.

Diritto di interruzione
Art. 31
[1]Chiunque può esigere dal titolare dell'elaborazione che:
a) un'elaborazione illecita di dati personali sia interrotta;
b) i dati personali raccolti, conservati o utilizzati in modo illecito siano distrutti e che le conseguenze della elaborazione illecita vengano eliminate;
c) i dati elaborati in modo illecito non vengano comunicati a terzi;
d) l'illegalità di un'elaborazione sia constatata.
[2]Il richiedente l'interruzione non deve dimostrare un interesse meritevole di tutela.

Diritti nei confronti di più organi
Art. 32
Se diversi organi utilizzano dati personali provenienti da un archivio di dati comune, la persona interessata può far valere i suoi diritti presso ogni organo.

Capitolo decimo
Vigilanza e rimedi giuridici

Incaricato cantonale della protezione dei dati
a) nomina, attribuzione e destituzione
Art. 33
[1]Il Consiglio di Stato nomina un Incaricato cantonale della protezione dei dati.
[2]L'Incaricato sottostà all'alta vigilanza del Gran Consiglio, il quale è competente per la conferma della nomina.
[3]L'Incaricato è attribuito amministrativamente alla Cancelleria dello Stato.
[4]L'Incaricato può essere sollevato dalle sue funzioni dal Gran Consiglio se è incapace di adempierle in modo permanente o se le viola intenzionalmente o per negligenza grave. Restano per il resto riservate le disposizioni della legge sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995 (LORD).

b) statuto
Art. 34
[1]L'Incaricato agisce in modo indipendente, senza ricevere né richiedere istruzioni.
[2]Non può esercitare attività incompatibili con la sua funzione e indipendenza.
[3]L'Incaricato svolge i suoi compiti di consulenza in modo gratuito per le persone e gli enti interessati.

c) risorse
Art. 35
[1]All'Incaricato sono attribuite adeguate risorse proprie, al fine di garantire l'efficace esecuzione dei suoi compiti di legge.
[2]L'Incaricato è coinvolto nella selezione del personale che si occupa della protezione dei dati.
[3]L'Incaricato presenta annualmente un progetto di preventivo che trasmette al Consiglio di Stato.

[4]L'Incaricato decide autonomamente, nei limiti del preventivo approvato dal Gran Consiglio, la gestione funzionale e operativa del servizio della protezione dei dati.

d) segreto d'ufficio
Art. 36
Rispetto alle informazioni riservate cui hanno accesso nell'adempimento delle loro funzioni e nell'esercizio dei loro poteri, l'Incaricato e il suo personale sono vincolati dallo stesso obbligo di riservatezza cui soggiace il titolare dell'elaborazione.

f) compiti
Art. 37
All'Incaricato cantonale della protezione dei dati sono attribuiti, segnatamente, i seguenti compiti:
a) sorveglia l'applicazione delle norme sulla protezione dei dati da parte dei soggetti sottoposti alla legge;
b) sorveglia l'applicazione della legge federale sulla protezione dei dati del 25 settembre 2020 (LPD);
c) sensibilizza i soggetti sottoposti alla legge sui loro doveri e le loro responsabilità di protezione dei dati e il pubblico in merito alle funzioni e alle attività dell'Incaricato, nonché ai diritti delle persone interessate e al loro esercizio;
d) è organo consultivo e di consulenza degli organi soggetti alla presente legge in materia di protezione e di sicurezza dei dati, in particolare sui progetti di elaborazione automatizzata di dati personali;
e) fa da intermediario fra persone interessate e gli organi responsabili;
f) in caso di violazione o di rischio di violazione delle prescrizioni legali in materia di protezione dati, invita l'autorità competente a prendere le misure necessarie;
g) esamina preliminarmente e preavvisa i progetti di atti legislativi e i provvedimenti rilevanti per la protezione dei dati, inclusi i trattamenti che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone;
h) esercita l'alta vigilanza in materia di protezione dei dati sui responsabili comunali della protezione dei dati;
i) presenta annualmente al Gran Consiglio e al Consiglio di Stato un rapporto nel quale commenta la propria attività; questo rapporto viene pubblicato;
j) collabora, nella misura necessaria allo svolgimento dei propri compiti, con le altre autorità di controllo dei Cantoni, della Confederazione e degli altri Paesi, in particolare scambiando con loro ogni informazione utile.
k) segue gli sviluppi determinanti per la protezione dei dati.

g) competenze e modo d'intervento
Art. 38
[1]L'Incaricato cantonale della protezione dei dati quale autorità di vigilanza e di controllo interviene di propria iniziativa o su segnalazione di terzi, se indizi lascino presumere che un'elaborazione di dati potrebbe essere contraria alle disposizioni sulla protezione dei dati.
[2]L'Incaricato tratta la segnalazione di terzi come denuncia all'autorità di sorveglianza e accerta i fatti d'ufficio. Egli informa la persona o l'organo segnalante sullo stato e sulle conclusioni dell'inchiesta entro congruo termine. Per il resto, la persona o organo segnalante non sono parte dell'inchiesta dell'Incaricato, a meno che la persona segnalante sia direttamente interessata dall'elaborazione di dati in questione. In tal caso, vanno

garantiti i diritti previsti dalla legge sulla procedura amministrativa del 24 settembre 2013 (LPAmm).
[3]Il titolare dell'elaborazione deve collaborare con l'Incaricato nello svolgimento delle sue funzioni, in particolare collaborare all'istruttoria. L'Incaricato può esigere dal titolare dell'elaborazione, dal responsabile dell'elaborazione, dai destinatari di dati o dalla persona interessata, informazioni orali o scritte riguardanti l'elaborazione di dati. Può consultare tutti i documenti e incarti relativi a determinate elaborazioni, effettuare ispezioni e chiedere la presentazione di elaborazioni nonché gli accessi ai loro sistemi informatici. All'Incaricato non può essere opposto il segreto d'ufficio o il segreto d'ufficio qualificato.
[4]Se dai chiarimenti risulta che sono state violate prescrizioni sulla protezione dei dati, l'Incaricato raccomanda al titolare dell'elaborazione di modificare, sospendere o cessare l'elaborazione. Egli informa della raccomandazione l'autorità superiore competente.
[5]Se interessi meritevoli di protezione di una persona sono in modo evidente minacciati o lesi, l'Incaricato può raccomandare al titolare dell'elaborazione o all'autorità superiore competente di limitare, sospendere o cessare immediatamente l'elaborazione dei dati personali.
[6]Il titolare dell'elaborazione o, se del caso, l'autorità superiore competente, dichiarano all'Incaricato, entro congruo termine definito da quest'ultimo, se intendono seguire la raccomandazione.
[7]Se una raccomandazione dell'Incaricato è respinta o non le è dato seguito, anche parzialmente, egli può decidere di far applicare tutta o parte della raccomandazione, se l'interesse alla sua messa in opera è preponderante. L'Incaricato può emettere direttamente una decisione se è prevedibile che il titolare dell'elaborazione rigetti la raccomandazione o non gli dia seguito.
[8]L'organo interessato o l'autorità superiore competente possono ricorrere, entro trenta giorni, contro la decisione dell'Incaricato alla Commissione cantonale della protezione dei dati.
[9]L'Incaricato, l'organo interessato o l'autorità superiore competente possono ricorrere contro la decisione della Commissione cantonale per la protezione dei dati e la trasparenza presso il Tribunale cantonale amministrativo.
[10]Se l'Incaricato non emette una decisione secondo il capoverso 7, egli può deferire la pratica per decisione alla Commissione cantonale della protezione dei dati e la trasparenza, nel caso in cui la raccomandazione è respinta o non le è dato seguito. La decisione della Commissione è comunicata con atto formale alla persona interessata e all'Incaricato.

Commissione cantonale per la protezione dei dati e la trasparenza
a) funzione e composizione
Art. 39
[1]Il Consiglio di Stato nomina ogni quattro anni una Commissione cantonale per la protezione dei dati e la trasparenza. Il Gran Consiglio ne conferma la nomina.
[2]La Commissione è indipendente. Essa si compone di un presidente e di quattro membri.
[3]La Commissione giudica nei casi previsti dalla legge.

b) competenze e procedura
Art. 40
[1]Ogni persona i cui dati sono elaborati dai soggetti sottoposti alla legge può far valere i diritti istituiti dalla presente legge chiedendo una decisione formale della Commissione cantonale per la protezione dei dati e la trasparenza.

[2]La richiesta di giudizio è fatta di regola come ricorso contro una decisione dell'organo che elabora i dati, o come denuncia contro quest'ultimo; l'organo che elabora i dati è parte nella procedura; il Consiglio di Stato può sempre intervenire come parte.
[3]La Commissione non è competente, se il ricorso contro la decisione è proponibile ad altro tribunale o istanza giudicante secondo una legge speciale, o se la domanda è già stata giudicata da un tribunale o da un'istanza giudicante.
[4]La Commissione può sospendere il giudizio per promuovere un tentativo di conciliazione.
[5]Le decisioni della Commissione sono impugnabili davanti al Tribunale cantonale amministrativo. Sono legittimati a ricorrere la persona dei cui dati si tratta, l'organo che elabora i dati e l'Incaricato cantonale della protezione dei dati.

Autorità di vigilanza comunali
Art. 41
I comuni possono nominare un responsabile della protezione dei dati, secondo le modalità previste dal regolamento di applicazione.

Capitolo undicesimo
Disposizioni penali

Contravvenzioni
Art. 42
Chiunque elabori dati personali su mandato e, intenzionalmente, non si attenga alle condizioni stipulate, è punito a querela di parte, con la multa sino a 10'000 franchi.

Capitolo dodicesimo
Disposizioni finali

Esecuzione
Art. 43
Il Consiglio di Stato emana le disposizioni di esecuzione della legge, in particolare riguardanti:
a) la sicurezza dei dati (art. 7 cpv. 7);
b) la responsabilità per la protezione dei dati (art. 8);
c) la protezione dei dati sin dalla progettazione (art. 14);
d) i progetti da sottoporre preventivamente all'Incaricato (art. 15 cpv. 2);
e) il contenuto della notifica della violazione della protezione dei dati all'Incaricato (art. 16);
f) la convenzione sulla protezione dei dati (art. 20 cpv. 2 lett. a e 21 cpv. 1);
g) le condizioni per l'interfacciamento di banche dati (art. 21 cpv. 3);
h) i registri degli archivi di dati (art. 26);
i) il diritto di accesso (art. 27);
j) l'organizzazione e la gestione della autorità cantonale di vigilanza (art. 33-38);
k) la nomina delle autorità comunali di vigilanza (art. 41).

Abrogazione
Art. 44
La legge sulla protezione dei dati personali del 9 marzo 1987 è abrogata.

Modifica di atti normativi
Art. 45

La modifica di atti normativi è disciplinata nell'allegato.

Entrata in vigore
Art. 46
[1]La presente legge sottostà a referendum facoltativo.
[2]Il Consiglio di Stato ne stabilisce la data di entrata in vigore.

Allegato di modifica di atti normativi

1.
La legge di applicazione della legge federale sull'armonizzazione dei registri e concernente la banca dati movimento della popolazione del 5 giugno 2000 è modificata come segue:

Capitolo quarto
Trasmissione di dati

Trasmissione di dati
a) tramite l'ufficio controllo abitanti e il Municipio
Art. 10a
[1]L'Ufficio controllo abitanti può trasmettere, su richiesta scritta, le indicazioni concernenti il cognome, il nome, il sesso, l'indirizzo, la data di arrivo e di partenza, la professione, il luogo di origine e la data di nascita di una singola persona, se l'istante fa valere un interesse legittimo.
[2]Il Municipio può trasmettere, sotto forma di lista, il cognome, il nome e l'indirizzo di persone aventi una o più caratteristiche comuni richieste dall'istante, se è garantita la loro utilizzazione unicamente per scopi ideali.
[3]Il Municipio può trasmettere altri dati su una singola persona, purché l'istante dimostri un interesse particolarmente meritevole di tutela.

b) tramite il Servizio cantonale del movimento della popolazione
Art. 10b
[1]Il Servizio cantonale del movimento della popolazione può trasmettere liste di dati personali per scopi ideali alle condizioni e modalità di cui all'articolo 10a capoverso 2.
[2]Per il resto, rimane riservata la trasmissione senza riferimento a persone specifiche secondo l'articolo 22 LPDP e l'assistenza amministrativa secondo il diritto speciale.

c) norme comuni
Art. 10c
La trasmissione di dati personali può essere limitata o sottoposta a condizioni qualora vi ostino importanti interessi pubblici o i dati si rivelino meritevoli di particolare protezione per la persona interessata.

Capitolo quinto
Disposizioni finali

2.
Nelle seguenti disposizioni, le espressioni «legge sulla protezione dei dati personali del 9 marzo 1987», «legge sulla protezione dei dati personali» e «legge sulla protezione dei dati personali (LPDP)» sono sostituite dall'espressione «legge sulla protezione dei dati personali del ……..…..…. (LPDP)»:
- art. 34a cpv. 5 della legge sulla cittadinanza ticinese e sull'attinenza comunale dell'8 novembre 1994 (LCCit);
- art. 12 cpv. 1 della legge sulle pubblicazioni ufficiali del 22 settembre 2014 (LPU);
- art. 3 cpv. 2 e art. 12 cpv. 2 della legge sull'informazione e sulla trasparenza dello Stato del 15 marzo 2011 (LIT);

- art. 2 cpv. 2 e art. 27 della legge sulla protezione dei dati personali elaborati dalla polizia cantonale e dalle polizie comunali del 13 dicembre 1999 (LPDPpol);
- art. 5 cpv. 5, art. 12 cpv. 1 e art. 13 cpv. 2 lett. d della legge sull'archiviazione e sugli archivi pubblici del 15 marzo 2011 (LArch);
- art. 84i della legge sull'ordinamento degli impiegati dello Stato e dei docenti del 15 marzo 1995 (LORD);
- art. 37 cpv. 2 della legge sugli aiuti allo studio del 23 febbraio 2015 (LASt);
- art. 4 cpv. 2 e art. 16 cpv. 1 della legge sulla statistica cantonale del 22 settembre 2009 (LStaC);
- art. 9b cpv. 5 e art. 9c cpv. 8 della legge sulla polizia del 12 dicembre 1989 (LPol);
- art. 39 cpv. 4 della legge sull'assistenza sociopsichiatrica del 2 febbraio 1999 (LASP);
- art. 22i cpv. 5 della legge di applicazione della legge federale sull'assicurazione malattie del 26 giugno 1997 (LCAMal);
- art. 2 cpv. 1 della legge sull'esercizio delle professioni di fiduciario del 1° dicembre 2009 (LFid).