Departement für Justiz, Sicherheit und Gesundheit Graubünden
Departament da giustia, segirezza e sanadad dal Grischun
Dipartimento di giustizia, sicurezza e sanità dei Grigioni

Revisione totale della legge cantonale sulla protezione dei dati (LCPD; CSC 171.100)

Rapporto esplicativo

Coira, novembre 2023

Indice

L'essenziale in breve

La legge cantonale sulla protezione dei dati (LCPD; CSC 171.100) è stata posta in vigore con effetto al 1° maggio 2002. In oltre venti anni, la legge è stata modificata soltanto in alcuni punti. Tuttavia, nello stesso arco di tempo la tecnologia ha fatto passi da gigante. Il calo dei prezzi degli spazi di archiviazione e la crescente disponibilità di connessioni internet sempre più veloci aprono possibilità molto più ampie rispetto al passato per ricevere, inviare e archiviare dati attraverso la rete. Inoltre, la dimensione transfrontaliera dei trattamenti di dati acquisisce un'importanza sempre maggiore. Per questi motivi, negli ultimi anni a livello europeo sono stati emanati o rivisti diversi atti normativi in materia di protezione dei dati. Questi atti normativi sono vincolanti anche per la Confederazione e i Cantoni e devono essere attuati nel diritto cantonale affinché le disposizioni cantonali sulla protezione dei dati soddisfino anche in futuro gli standard europei. In tal modo rimane garantito l'accesso al Sistema d'informazione Schengen (SIS), in particolare per il lavoro di polizia. Occorre dunque procedere a una revisione totale della LCPD, limitandosi a quei punti che sono assolutamente necessari per attuare le disposizioni di diritto internazionale. Gli organi pubblici soggetti alla legge sono tenuti a impiegare alcuni nuovi strumenti e a soddisfare alcuni nuovi obblighi concepiti principalmente per rafforzare i diritti delle persone i cui dati sono oggetto di trattamento. Inoltre, il diritto di rango superiore richiede un rafforzamento della vigilanza sulla protezione dei dati che nel Cantone dei Grigioni viene assunta dall'incaricato della protezione dei dati. La revisione legislativa punta da un lato a rafforzare l'autonomia di quest'organo, dall'altro a conferirgli nuovi compiti e competenze.

I. Situazione di partenza

1. Sviluppi nel diritto internazionale e federale

Il diritto sulla protezione dei dati si propone di tutelare la personalità delle persone i cui dati sono oggetto di trattamento e di garantire così l'autodeterminazione informativa ai sensi dell'art. 13 cpv. 2 della Costituzione federale della Confederazione svizzera (Cost.; RS 101). Secondo questa disposizione, ognuno ha diritto d'essere protetto da un impiego abusivo dei suoi dati personali. A livello federale, l'art. 13 cpv. 2 Cost. viene concretizzato in primo luogo dalla legge federale sulla protezione dei dati (LPD; RS 235.1). Quest'ultima si applica soltanto al trattamento di dati personali da parte di organi federali e di privati (art. 1 LPD). I Cantoni sono dunque chiamati a emanare leggi proprie che disciplinano il trattamento di dati da parte di organi pubblici cantonali, comunali o regionali. Per tale ragione, il Cantone dei Grigioni ha posto in vigore una legge cantonale sulla protezione dei dati (LCPD; CSC 171.100) con effetto al 1° maggio 2002. In quanto «diritto formale in materia di protezione dei dati», la LCPD disciplina anzitutto i principi e le direttive generali concernenti i trattamenti di dati da parte delle autorità. La tipologia di dati che può essere trattata nei rispettivi ambiti giuridici risulta dalle prescrizioni concernenti il trattamento di dati contenute nel rispettivo diritto specifico del settore («diritto materiale in materia di protezione die dati»). Questo può essere il diritto cantonale o federale.

Negli oltre vent'anni trascorsi dall'entrata in vigore della LCPD la tecnologia ha compiuto passi da gigante. Il numero di dispositivi e applicazioni che producono ed elaborano dati è

notevolmente aumentato. Il calo dei prezzi degli spazi di archiviazione e la crescente disponibilità di connessioni internet sempre più veloci aprono possibilità molto più ampie rispetto al passato per ricevere, inviare e archiviare dati attraverso la rete. Inoltre, la dimensione transfrontaliera dei trattamenti di dati acquisisce un'importanza sempre maggiore. Di conseguenza sono state definite determinate direttive transfrontaliere sul trattamento di dati. Vanno menzionati, tra gli altri, il regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (regolamento generale sulla protezione dei dati, di seguito GDPR) e la direttiva (UE) 2016/680 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 (di seguito: direttiva 2016/680), entrambi approvati dal Parlamento europeo e dal Consiglio dell'Unione europea nell'aprile 2026. La direttiva 2016/680 disciplina esclusivamente la cooperazione di polizia e giudiziaria. Il GDPR invece si applica in linea di principio a tutti i trattamenti di dati. Mentre la direttiva 2016/680, quale parte dell'acquis di Schengen, deve essere attuata nel diritto interno a livello di Confederazione e Cantoni, il GDPR non è un ulteriore sviluppo dell'acquis di Schengen e non deve dunque essere recepito nel diritto nazionale. Ciononostante, il GDPR è comunque importante perché, secondo il diritto in materia di protezione dei dati, per l'UE la Svizzera è uno Stato terzo e la Commissione europea decide periodicamente in virtù delle disposizioni del GDPR se la legislazione dei Paesi terzi garantisce un livello adeguato di protezione dei dati. La decisione di adeguatezza consente la possibilità di trasferire dati da o verso i Paesi dell'UE senza ulteriori restrizioni o misure particolari. Per la Svizzera, alcuni standard minimi per la protezione dei dati derivano anche dalla Convenzione europea sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale del 28 gennaio 1981 (Convenzione STE 108; RS 0.235.1) e dal suo protocollo aggiuntivo dell'8 novembre 2001 (RS 0.235.11). Questa Convenzione è stata riveduta dal Consiglio d'Europea contemporaneamente alle normative sopra citate. Dal punto di vista contenutistico la Convenzione STE 108 si orienta alla direttiva 2016/680. A differenza della direttiva 2016/680, la Convenzione STE 108 è tuttavia applicabile a tutti i trattamenti di dati. Con il decreto federale del 19 giugno 2020, le Camere federali hanno autorizzato il Consiglio federale a ratificare la Convenzione riveduta. Con la ratifica della Convenzione, la Confederazione e i Cantoni si sono impegnati a procedere ai necessari adeguamenti nella loro legislazione in materia di protezione dei dati al fine di garantire il rispetto degli standard minimi sanciti dalla Convenzione STE 108.

A seguito delle disposizioni del diritto internazionale e delle condizioni quadro tecnologiche e sociali, la LPD federale è stata sottoposta a revisione totale. Per motivi di tempo, il progetto di legge è stato diviso in due parti: in una prima fase il Consiglio nazionale e il Consiglio degli Stati hanno approvato, nel mese di settembre 2018, il decreto federale concernente il recepimento della direttiva UE 2016/680 nonché le modifiche legislative necessarie all'attuazione di questa direttiva. Questa parte della legge rivista è entrata in vigore il 1° marzo 2019. Le restanti parti della revisione totale della legge federale sulla protezione dei dati presentate dal Consiglio federale sono state approvate dalle Camere federali il 25 settembre 2020. La nuova LPD nella versione integralmente rivista è entrata in vigore il 1° settembre 2023.

2. Necessità di revisione

La necessità di rivedere il diritto in materia di protezione dei dati è legata in primo luogo agli sviluppi tecnologici degli ultimi vent'anni. La risultante necessità di modifica, rilevante ai fini di una protezione efficace dell'autodeterminazione informativa, è stata individuata negli sviluppi a livello di diritto internazionale, che, secondo quanto esposto sopra, sono importanti anche per la Svizzera, ed è stata attuata. Il Cantone dei Grigioni è chiamato a procedere ai relativi adeguamenti necessari in base alla direttiva 2016/680 e alla Convenzione STE 108. Le disposizioni del diritto internazionale prevedono nuovi strumenti e obblighi che devono trovare attuazione nel diritto cantonale. Viene inoltre prescritto un rafforzamento dello statuto e delle competenze dell'organo di vigilanza cantonale in materia di protezione dei dati. La rilevanza della LPD completamente riveduta della Confederazione, entrata in vigore il 1° settembre 2023, deriva dal fatto che, attraverso una serie di singoli rimandi dinamici (cfr. art. 1 cpv. 4, art. 2 cpv. 2 e 3, art. 4 cpv. 2 e art. 5 cpv. 3 LCPD), l'attuale LCPD dichiara questa legge applicabile per analogia. A seguito di questi rimandi, con la sua entrata in vigore la LPD è sostanzialmente diventata diritto cantonale vigente e quindi diversi adeguamenti richiesti dal diritto internazionale sono già stati attuati a livello giuridico. Nel frattempo, nel quadro della revisione totale della LPD sono state modificate anche la struttura dell'atto normativo e alcune importanti definizioni di concetti chiave. Per tale motivo non è più sempre chiaro a quali disposizioni si riferiscano i singoli rimandi. Tuttavia, è proprio questo aspetto che rappresenta un presupposto importante per l'ammissibilità di rimandi dinamici del diritto cantonale al diritto federale (cfr. DTF 134 I 179 consid. 6.3.). Si deve partire dal presupposto che gli attuali rimandi contenuti nella LCPD non bastino più per incorporare in modo sufficientemente chiaro nel diritto cantonale tutte le modifiche necessarie. In alcuni punti, peraltro, il diritto federale si spinge oltre le disposizioni del diritto internazionale. Se a seguito degli attuali rimandi queste disposizioni vengono riprese senza alcuna restrizione, tali obblighi devono essere attuati integralmente anche nel Cantone dei Grigioni. In questi casi il Cantone non sfrutterebbe il margine di manovra che gli è stato concesso e rinuncerebbe alla possibilità di emanare normative proprie adeguate alle caratteristiche cantonali. Ad esempio, secondo la LPD tutti gli enti pubblici sono obbligati a tenere un registro delle attività di trattamento o a designare un consulente per la protezione dei dati (cfr. sotto, art. 22 e 23). Nel Cantone dei Grigioni questi obblighi si applicherebbero quindi anche ai comuni e alle regioni. Questo non è tuttavia l'obiettivo perseguito. Inoltre, gli art. 7-10 della LCPD disciplinano lo statuto e le competenze dell'organo di vigilanza e dell'incaricato della protezione dei dati senza fare riferimento alla legge federale. Anche queste disposizioni devono essere modificate affinché corrispondano alle disposizioni del diritto internazionale. Risulta quindi necessaria una revisione della LCPD.

II. Assetto e tratti fondamentali del progetto di legge

1. Spiegazioni di carattere generale

Negli art. 1 cpv. 4, art. 2 cpv. 2 e 3, art. 4 cpv. 2 e art. 5 cpv. 3 la LCPD vigente rimanda alle relative disposizioni in materia della LPD. In sede di elaborazione della presente legge, il legislatore ha scelto questo sistema caratterizzato da una combinazione di diversi singoli rimandi e di regolamentazioni proprie per riprendere le normative della legge federale senza ripetere le relative disposizioni. Grazie a tali rimandi, la LCPD risulta più snella rispetto ad altri atti normativi sulla protezione dei dati. A questo vantaggio si contrappone il grosso svantaggio che la legge non è comprensibile di per sé. Tuttavia, grazie ai rimandi in caso di controversie è possibile prendere a riferimento i materiali relativi alla legislazione federale nonché la giurisprudenza e la letteratura pertinenti. Per questo motivo, finora le parti coinvolte considerano i rimandi dinamici come funzionali/idonei. Con la revisione totale della LPD sono cambiate la sistematica e la definizione di diversi termini. Questi adeguamenti apportati all'oggetto cui si rimanda fanno sì che in determinate circostanze non è più chiaro se determinate disposizioni della LPD hanno senz'altro validità anche nel diritto cantonale. Inoltre, in questo modo il Cantone riprende determinati obblighi e strumenti previsti dal diritto federale che risultano più stringenti rispetto alle disposizioni del diritto internazionale di cui alla direttiva 2016/680 e alla Convenzione STE 108 (cfr. cap. I.2.). Questo approccio risulta ulteriormente complicato dal fatto che le modifiche interessano componenti essenziali del diritto formale in materia di protezione dei dati del Cantone, senza che a livello cantonale le modifiche siano state soggette ad alcuna procedura legislativa. Nel presente contesto, questa circostanza è particolarmente svantaggiosa in quanto a essere interessati sono in linea di principio tutti i processi di diritto amministrativo a livello cantonale, regionale e comunale che comportano il trattamento di dati personali. La revisione intende evitare che agli organi pubblici soggetti alla legislazione sulla protezione dei dati vengano imposti obblighi che vanno oltre quanto previsto dal diritto internazionale. Il Governo vuole quindi sfruttare il margine di manovra a disposizione del Cantone. A questo scopo occorre adeguare ampiamente i rimandi dinamici o sostituirli con una regolamentazione propria. In caso di semplice adeguamento dei rimandi potrebbero insorgere nuove difficoltà interpretative. Inoltre, in occasione della prossima revisione generale della legge federale si riproporrebbero gli stessi problemi.

Per i motivi menzionati, i rimandi dinamici dovranno essere sostituiti da una regolamentazione propria. Ciò non significa che i requisiti posti al trattamento dei dati saranno più severi rispetto a quanto previsto dal diritto vigente. Nuovi obblighi o strumenti verranno creati solo laddove ciò risulta necessario a seguito del diritto internazionale. Con i rimandi dinamici, per numerose questioni giuridiche si è potuto fare capo ai materiali, alla giurisprudenza e alla letteratura della legge federale sulla protezione dei dati, facilitando l'interpretazione della LCPD da parte di chi applica il diritto a livello cantonale. Questa possibilità deve essere preservata incorporando nella versione rivista della legge sulla protezione dei dati i contenuti di numerose disposizioni della LPD senza modifiche materiali. A questa circostanza si fa riferimento più volte anche nelle spiegazioni relative alle singole disposizioni. In questo contesto occorre richiamare l'attenzione sul fatto che solo nel Cantone di Obvaldo la legislazione sulla protezione dei dati rimanda alla normativa federale in misura analogamente ampia a quanto fa il Cantone dei Grigioni. Tutti gli altri Cantoni hanno optato per una regolamentazione propria.

Spesso, attraverso formulazioni concordanti o corrispondenti rinvii nei materiali anche loro consentono il ricorso esplicito o implicito ai materiali della Confederazione e ai principi sviluppati a tale scopo dalla giurisprudenza e dalla dottrina.

Occorre tenere presente che la LPD riveduta è entrata in vigore il 1° settembre 2023. A seguito dei rimandi dinamici, al momento della consultazione essa rappresenta sostanzialmente il diritto cantonale applicabile. Per ragioni di chiarezza e leggibilità, si presume che la LPD nel suo insieme rappresenti il diritto applicabile, sebbene secondo quanto esposto sinora non sia chiaramente dimostrato se i singoli rimandi inglobino tutti i nuovi strumenti. Il testo del presente progetto di legge continua a basarsi sostanzialmente sulla LPD, al fine di continuare a consentire l'uso dei materiali. Nelle spiegazioni si sottolinea più volte questo aspetto ed eventuali deroghe vengono motivate. Siccome non si può presumere che tutti i destinatari conoscano nel dettaglio le differenze tra la vLPD in vigore fino al 1° settembre 2023 e la versione successiva alla revisione totale, nel quadro delle spiegazioni vengono esplicitate le discrepanze rilevanti tra la vecchia e la nuova legge federale.

2. Modifiche più importanti

Con la revisione totale della legge, attraverso diversi nuovi strumenti e obblighi introdotti, il livello di protezione dei dati risulta accresciuto così come richiesto dalla legge di rango superiore. L’esigenza di intervenire, resasi necessaria a livello cantonale per effetto della direttiva 2016/680 e della Convenzione STE 108, è stata riassunta in una guida dalla Conferenza dei governi cantonali (CdC) con la significativa collaborazione di rappresentanti delle autorità cantonali preposte alla vigilanza della protezione dei dati (di seguito: guida CdC). Questa guida funge da base per la revisione che si limita in ampia misura alla necessità assoluta, comprovata in questa guida, di procedere ad adeguamenti al fine di attuare il diritto europeo modificato in materia di protezione dei dati. In questo contesto vengono introdotti alcuni nuovi strumenti e obblighi richiesti dal diritto internazionale che da un lato servono agli stessi organi pubblici, dall'altro sono intesi a rafforzare lo statuto delle persone interessate. La legge rafforza inoltre lo statuto dell'organo di vigilanza cantonale in materia di protezione dei dati per quanto riguarda le sue competenze e la sua indipendenza. Inoltre la terminologia della LCPD viene adeguata a quella della LPD e alle disposizioni del diritto internazionale e in alcuni casi completata con nuovi termini.

Di seguito sono riportate le modifiche più importanti. A causa dei rimandi dinamici al diritto federale, alcune delle modifiche qui elencate devono essere trattate come diritto vigente sin dall'entrata in vigore della revisione totale della LPD. Poiché rispetto alla situazione giuridica in essere, tali modifiche rappresentano un'importante novità, occorre comunque presentarle in questa sede:

- a titolo di novità l'organo pubblico titolare del trattamento deve essere in grado di dimostrare nei confronti dell'organo di vigilanza il rispetto delle disposizioni in materia di protezione dei dati;
- se un organo pubblico titolare del trattamento intende procedere a un trattamento di dati personali che presumibilmente comporta un rischio elevato per i diritti fondamentali della persona interessata, esso deve effettuare una valutazione d'impatto sulla protezione dei dati (già in atto in virtù dell'art. 22 LPD);

- in specifici casi in cui il trattamento di dati personali comporta un rischio elevato per i diritti fondamentali delle persone interessate sussiste l'obbligo di chiedere previamente il parere dell'organo di vigilanza (già in atto in virtù dell'art. 23 LPD);
- eventuali violazioni delle disposizioni sulla protezione dei dati devono essere notificate quanto prima all'organo di vigilanza; a determinate circostanze, tale obbligo di notifica va esteso anche alle persone interessate (già in atto in virtù dell'art. 24 LPD);
- gli organi coinvolti nell'attuazione dell'acquis di Schengen (polizia, Procura pubblica, ecc.) sono obbligati a tenere un registro delle rispettive attività di trattamento o a designare un consulente per la protezione dei dati (gli art. 10 e 12 LPD lo prevedono per tutti gli organi pubblici, nel Cantone quest'obbligo deve valere soltanto per gli organi coinvolti nell'attuazione dell'acquis di Schengen);
- le competenze dell'organo cantonale di vigilanza in materia di protezione dei dati vengono ampliate, rafforzando in tal modo il suo statuto. In futuro, tale autorità non solo potrà formulare raccomandazioni relative al trattamento di dati a destinazione degli organi pubblici soggetti alla sua vigilanza, ma potrà anche emanare, come «ultima ratio», decisioni impugnabili nei loro confronti;
- l'indipendenza istituzionale dell'incaricato della protezione dei dati viene rafforzata, tra l'altro anche attraverso l'introduzione di un sistema di elezione per un mandato con possibilità di destituzione dalla carica soltanto in caso di incapacità permanente di esercitare la carica o di grave violazione dei doveri d'ufficio.

III. Spiegazioni relative alle singole disposizioni

Art. 1 Scopo

Come già sancito nell'art. 1 LCPD in vigore, la legge serve a proteggere le persone dal trattamento illecito di dati personali da parte di organi pubblici.

Art. 2 Campo d'applicazione

Questo articolo disciplina il campo di applicazione della LCPD. Come finora, la legge si applica al trattamento di dati personali da parte di organi pubblici. Va mantenuta l'eccezione, già prevista precedentemente, al campo d'applicazione, se un organo pubblico prende parte alla concorrenza economica e in questo ambito non agisce in veste decisionale. I relativi trattamenti di dati si conformano alla LPD. Poiché tuttavia gli organi pubblici non diventano privati, bensì agiscono soltanto come tali, l'organo di vigilanza cantonale rimane competente per la vigilanza. Non sarà più necessaria l'eccezione prevista dall'art. 1 cpv. 5 lett. b della LCPD in vigore relativa ai dati personali conservati in un archivio pubblico. In questo caso prevalgono le disposizioni pertinenti della legge sulla gestione degli atti e sull'archiviazione (LGAA; CSC 490.000), nel frattempo posta in vigore, in quanto normativa di diritto materiale in materia di protezione dei dati (cfr. cpv. 4). Finora, altri motivi di esclusione si applicavano sulla base del rimando al diritto federale (art. 1 cpv. 4 LCPD). I motivi di esclusione di cui all'art. 2 cpv. 2 LPD (uso privato, beneficiari istituzionali) incorporati in questo modo sono solo parzialmente pertinenti in relazione al trattamento da parte di organi pubblici e non vengono dunque mantenuti nel quadro della revisione.

In base al diritto internazionale, non saranno più ammesse eccezioni generali al campo di

applicazione della legge sulla protezione dei dati per procedimenti dell'amministrazione della giustizia civile e penale e per procedure della giurisdizione amministrativa giudiziaria. Ciò non vuole dire che non si applicheranno più i codici di diritto processuale. Le norme pertinenti contenute in queste leggi (ad es. nel Codice di diritto processuale penale svizzero [CPP; RS 312.0]) rimarranno valide in quanto diritto settoriale in materia di protezione dei dati e le regole in esse statuite (ad es. relative alla consultazione degli atti) prevarranno sulla LCPD. I principi sanciti dalla legge sulla protezione dei dati si applicheranno invece in via sussidiaria. L'art. 2 cpv. 3 LCPD riprende in gran parte la formulazione della legge federale (art. 2 cpv. 3 LPD). Nei procedimenti dinanzi ai giudici penali e civili si applicheranno gli ordinamenti procedurali pertinenti della Confederazione. Oltre alla normativa federale, nella LCPD devono essere citate le procedure di giurisdizione amministrativa in cui i diritti sono disciplinati dalla legge cantonale sulla giustizia amministrativa (LGA; CSC 370.100). Per le procedure amministrative di prima istanza, il trattamento dei dati sarà retto esclusivamente dalla LCPD, in deroga a quanto indicato sinora e come già previsto dalla precedente legge.

Art. 3 Definizioni

La LPD e la maggior parte delle leggi cantonali sulla protezione dei dati contengono una disposizione indicante le principali definizioni legali. Con la rinuncia ai rimandi dinamici, anche nella LCPD deve essere aggiunta una disposizione di questo tipo che si orienta in ampia misura alla disposizione della legge federale (art. 5 LPD). Le seguenti definizioni si discostano dalla legge federale:

- Il cpv. 1 definisce il concetto di organo pubblico, circoscrivendo così il campo di applicazione materiale della legge. Per le definizioni concettuali ci si conforma alla legge sul principio di trasparenza (legge sulla trasparenza; CSC 171.000), senza che ciò comporti modifiche del quadro giuridico. Come secondo il diritto vigente, la legge si rivolge alle autorità del Cantone, delle regioni e dei comuni nonché alle relative istituzioni, fondazioni e corporazioni, tra cui, per esempio, anche i comuni patriziali e parrocchiali. La legge si applica anche a privati che svolgono compiti pubblici loro delegati.

- Il cpv. 2 definisce il concetto di dati personali. Esso si discosta dalla legge federale nella misura in cui la LCPD continuerà a proteggere i dati concernenti sia le persone fisiche che giuridiche. In virtù del principio di legalità, abrogare l'applicabilità della LCPD ai dati concernenti persone giuridiche significherebbe escludere questi ultimi da tutte le disposizioni di diritto materiale in materia di protezione dei dati con le quali attualmente gli organi pubblici vengono autorizzati a trattare dati personali. Di conseguenza andrebbero adeguate tutte le leggi speciali. La Confederazione ha scelto di seguire questa strada, disciplinando nella legge federale sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS 172.010) i principi applicabili al trattamento di dati concernenti persone giuridiche da parte di organi federali. Per il momento, le basi legali vigenti consentono il trattamento concreto di dati concernenti persone giuridiche in virtù di una disposizione transitoria contenuta nell’art. 71 LPD. Inoltre viene prospettata un'ampia revisione dell'ordinamento legislativo incentrata sulla definizione dei settori in cui dovrà continuare a essere possibile il trattamento di dati concernenti

persone giuridiche. Poiché i nuovi principi stabiliti nella LOGA corrispondono in ampia misura a quelli della legge sulla protezione dei dati, questo approccio non rafforza né indebolisce il livello di protezione dei dati concernenti persone giuridiche, che peraltro generalmente ha rilevanza autonoma solo limitata. Nel Cantone dei Grigioni è dunque previsto che la LCPD continui a tutelare anche i dati concernenti persone giuridiche, per mantenere una prassi che si dimostrata valida.

Inoltre sono stati conformati al diritto federale e al diritto internazionale anche i seguenti termini:

- Il cpv. 3 riprende l'elenco dei dati personali degni di particolare protezione stabilito nella legge federale (art. 5 lett. c LPD). Rientrano in tale elenco, ad esempio, i dati concernenti la religione, la salute o le sanzioni amministrative e penali. Rispetto alla situazione giuridica in essere, in virtù delle disposizioni del diritto internazionale anche i dati genetici e biometrici che identificano in modo univoco una persona devono essere indicati esplicitamente come dati personali degni di particolare protezione.

- Rispetto al diritto vigente, sulla base delle disposizioni del diritto internazionale a titolo di novità deve essere disciplinata la profilazione. La definizione del termine è stata ripresa dalla legge federale, con la differenza che la LCPD mantiene l'applicabilità sui dati concernenti sia le persone fisiche che giuridiche. A differenza del diritto federale, nell'ordinamento giuridico cantonale dovrà essere mantenuto il termine di profilo della personalità (art. 3 lett. d vLPD). La ragione risiede nel fatto che il termine utilizzato in diverse leggi speciali non può essere sostituito con il concetto di profilazione in tutti i singoli casi (cfr. ad es. art. 24 legge sulla cittadinanza del Cantone dei Grigioni [LCCit; CSC 130.100]).

- Il termine «collezione di dati» (art. 3 lett. g vLPD) non compare più nella LPD e di conseguenza non viene più utilizzato neanche nella LCPD. Di conseguenza viene sostituito anche il termine «detentore di una collezione di dati» (art. 3 lett. i vLPD; vedi il successivo art. 4).

- A titolo di novità viene introdotta una definizione legale basata sull'art. 5 lett. k nLPD per «responsabile del trattamento».

Art. 4 Responsabilità

L'attribuzione della responsabilità nell'ambito della protezione dei dati costituisce un pilastro centrale del diritto in materia di protezione dei dati. Secondo il cpv. 1, per la protezione dei dati è responsabile l'organo pubblico che, singolarmente o insieme ad altri, determina lo scopo e i mezzi del trattamento. In questo modo viene ripresa la definizione di «titolare del trattamento» ai sensi dell'art. 5 lett. j LPD, che a sua volta sostituisce senza modifica materiale il termine «detentore di una collezione di dati». In caso di trattamento congiunto di dati da parte di più organi, la responsabilità deve essere disciplinata tra questi organi. La regolamentazione vigente conformemente al rimando alla legge federale secondo la quale, in questi casi, spetta al Governo dover disciplinare la responsabilità (art. 2 cpv. 2 LCPD in unione

con l'art. 33 LPD), non è mai stata applicata nella prassi e non risulta di utilità. In futuro spetterà invece agli organi coinvolti definire quale tra questi organi si assumerà quale parte della responsabilità nell'ambito della legge sulla protezione dei dati. In particolare, occorrerà definire quale tra gli organi coinvolti assumerà la responsabilità generale per il trattamento di dati in questione. In base alle disposizioni del diritto di rango superiore l'organo pubblico dovrà dimostrare all'incaricato della protezione dei dati di aver rispettato le disposizioni sulla protezione dei dati. La modalità in cui ciò dovrà avvenire potrà essere definita a livello di ordinanza. È ad esempio ipotizzabile che a tale scopo vengano utilizzati i risultati della valutazione d'impatto sulla protezione dei dati (art. 19) o del registro delle attività di trattamento (art. 22).

Art. 5 Principi del trattamento di dati

L'art. 5 intende disciplinare i principi essenziali del trattamento di dati. L'attuale art. 2 cpv. 1 LCPD stabilisce che il trattamento di dati personali deve rispettare i principi della legalità, della proporzionalità, dell'adeguatezza, della destinazione vincolata, dell'esattezza e della sicurezza dei dati. In virtù del rimando contenuto nell'art. 2 cpv. 2 LCPD, la concretizzazione di questi principi e l'inclusione di eventuali altri principi avvengono tramite il diritto federale. Con la rimozione del rimando, questi principi verranno ora sanciti nella legge stessa. La descrizione dei principi viene ripresa dall'art. 6 LPD. Eventuali adeguamenti rispetto alla vecchia LPD sono in primo luogo di natura terminologica e non comportano alcuna modifica della situazione giuridica.

Art. 6 Sicurezza dei dati

Spetta all'organo pubblico titolare del trattamento o al responsabile del trattamento garantire, mediante appropriati provvedimenti tecnici e organizzativi, che la sicurezza dei dati personali sia adeguata al rischio. La relativa disposizione è stata ripresa senza variazioni significative dalla legge federale (art. 2 cpv. 2 LCPD in unione con l'art. 8 LPD). Il cpv. 2 stabilisce che l'obiettivo dei provvedimenti deve sempre essere quello di evitare violazioni della sicurezza dei dati. La natura dei provvedimenti tecnici e organizzativi adottati nel singolo settore segue, come nel diritto federale, un approccio basato sul rischio. Quanto maggiore è il rischio di violazione della sicurezza dei dati, tanto più severi sono i requisiti posti ai provvedimenti da adottare. I provvedimenti saranno dunque commisurati alla relativa necessità di protezione. Nel cpv. 3 il Governo viene autorizzato a concretizzare i corrispondenti requisiti minimi a livello di ordinanza. A tale riguardo dovrà essere possibile divergere dalle condizioni severe dell'ordinanza relativa alla legge federale sulla protezione dei dati (OLPD; RS 235.11) attualmente vigenti in forza del rimando dinamico.

Art. 7 Trattamento di dati personali

Come finora, il trattamento di dati personali ad opera di organi pubblici è consentito in primo luogo in virtù di una base legale. Una tale base giuridica può essere costituita da un obbligo o da un'autorizzazione espliciti a un determinato trattamento di dati (cosiddetta base legale diretta, cfr. ad es. l'art. 24 LCCit che autorizza espressamente le autorità competenti al trattamento di dati) oppure da un compito legale per il cui adempimento sono necessari specifici trattamenti di dati (cosiddetta base legale indiretta, cfr. ad es. l'art. 123 della legge federale sull'imposta federale diretta [LIFD; RS 642.11] o l'art. 130a della legge sulle imposte per il

Cantone dei Grigioni [LIG; CSC 720.000]). In questo contesto viene ripresa in ampia misura la disposizione pertinente della LPD (art. 34 LPD). Tuttavia, il diritto grigionese non conosce i termini di legge in senso formale/materiale utilizzati in tale atto normativo. Per questo motivo, al fine di garantire l'uniformità dell'ordinamento giuridico del Cantone, nella LCPD si parlerà di legge (formale) e di ordinanza (materiale). Il cpv. 4 fissa i presupposti che legittimano in via generale la rinuncia a una base legale. Ciò avviene quando la persona interessata ha dato, nel caso specifico, il suo consenso al trattamento (per il consenso, cfr. sopra art. 5) oppure ha reso i suoi dati personali accessibili a chiunque e non si è opposta espressamente al trattamento. In deroga al vecchio diritto e in conformità al diritto internazionale è prevista inoltre un'eccezione quando il trattamento è necessario per proteggere la vita o l'integrità fisica della persona interessata o di un terzo e non è possibile ottenere il consenso della persona interessata entro un termine ragionevole. Occorre tenere presente che queste eccezioni valgono esplicitamente per il caso concreto e non giustificano il trattamento ininterrotto di dati in assenza di una base legale.

Rispetto alla legge attualmente in vigore risultano le seguenti modifiche e concretizzazioni. Poiché a titolo di novità la profilazione (cfr. sopra art. 2 cpv. 5 LCPD) è disciplinata quale tipo di trattamento di dati degno di particolare protezione, per i relativi trattamenti di dati deve essere prevista una specifica base legale. Inoltre, in conformità alla regolamentazione federale, viene creata una fattispecie residuale per i trattamenti di dati che, pur non rientrando né nella profilazione né nel profilo della personalità, possono comunque determinare una grave ingerenza nei diritti fondamentali della persona interessata per via dello scopo e delle modalità di trattamento. In deroga al cpv. 2, se i presupposti di cui al cpv. 3 sono soddisfatti in via cumulativa sarà sufficiente una base legale a livello di ordinanza. In futuro si rinuncia alla possibilità concessa al Governo di autorizzare un trattamento di dati in assenza di una base legale quando ritiene che i diritti della persona interessata non siano a rischio. A quanto risulta, questa eccezione non è mai stata applicata. Essa può perciò essere abrogata.

Art. 8 Trattamento automatizzato di dati personali nell'ambito di sistemi pilota

Il diritto vigente prevede già, in virtù dell'art. 35 LPD, determinate agevolazioni soprattutto a livello di basi legali per quanto riguarda il trattamento automatizzato di dati personali degni di particolare protezione e profili della personalità nell'ambito di sistemi pilota. La disposizione consente di sperimentare gli accessi a collezioni di dati prima che venga emanata una base legale formale, così da poter determinare l'adeguatezza e la necessità dell'accesso nonché l'esigenza di una regolamentazione. In tal modo si tiene conto del fatto che di norma il processo legislativo dura due anni. Così può succedere che in determinate circostanze un progetto normativo risulti già superato per via dei progressi tecnologici e che non risponda più alle effettive esigenze. Questa possibilità va mantenuta proprio in vista dell'intensificazione della digitalizzazione dell'amministrazione. La disposizione dell'art. 35 LPD viene ripresa per analogia.

Art. 9 Trattamento da parte di un responsabile del trattamento

L'art. 9 disciplina il trattamento di dati da parte di un responsabile del trattamento. Nella prassi il cosiddetto «outsourcing» è di grande importanza perché, ad es., per definizione (cfr. sopra art. 3) la semplice archiviazione di dati su un servizio cloud è considerata come trattamento di dati. Il diritto vigente rimanda in sostanza alle regolamentazioni pertinenti della Confederazione (art. 9 LPD) e nell'art. 3 cpv. 2 LCPD prevede inoltre la necessità del previo consenso in caso di affidamento a terzi del trattamento da parte del responsabile del trattamento (cosiddetto «subcontracting»). Questa disposizione viene sostanzialmente ripresa. Di conseguenza il trattamento di dati personali può essere affidato per contratto o per legge a un responsabile del trattamento, se i dati vengono trattati secondo le modalità di trattamento concesse allo stesso organo pubblico titolare del trattamento e se nessun obbligo legale o contrattuale di serbare il segreto vieta l'affidamento.

In relazione all'outsourcing occorre inoltre tenere conto dell'art. 7 della futura legge sull'amministrazione digitale (LADig; CSC 177.100)[1] che sancisce alcuni requisiti generali per l'esternalizzazione di trattamenti di dati e la gestione di soluzioni informatiche da parte di terzi. Le autorità amministrative cantonali dovranno soddisfare i requisiti minimi di cui all'art. 7 LADig per tutte le attività di trattamento che esternalizzano. L'art. 9 LCPD si applica invece a tutti gli organi pubblici soggetti alla LCPD. Il suo campo di applicazione è più ristretto poiché limitato al trattamento di dati personali. L'art. 7 LADig rimanda alle disposizioni della legislazione sulla protezione dei dati nella misura in cui il mandatario è tenuto a rispettare i medesimi requisiti rispettati da essa stessa per quanto riguarda la protezione dei dati nonché la sicurezza dei dati e d'esercizio. In tal caso i requisiti specifici posti alla protezione dei dati si conformano all'art. 9 LCPD. Inoltre è possibile che sussistano requisiti posti alla sicurezza dei dati e d'esercizio che le autorità pubbliche devono rispettare in virtù dell'art. 7 LADig. Come requisito per tutti i trattamenti di dati, l'art. 7 LADig prevede inoltre che l'adempimento dei compiti statali venga il meno possibile pregiudicato nel caso in cui il mandatario non rispetti gli accordi stipulati o cessi la propria attività. Sia l'art. 7 LADig sia l'art. 9 LCPD richiedono una base per il trattamento di dati (ad es. sotto forma di una regolamentazione legislativa o di un contratto). Il contenuto della relativa base sarà concretizzato a livello di ordinanza.

Art. 10 Comunicazione di dati personali 1. Direttive generali

L'art. 10 disciplina le condizioni generali alle quali gli organi pubblici possono comunicare dati personali. Anche in questo caso viene ripreso in ampia misura il diritto federale (art. 36 LPD), con modifiche soltanto lievi della situazione giuridica attuale. Per la comunicazione di dati personali continuerà a essere necessaria in primo luogo una base legale che rispetti gli stessi requisiti richiesti per il trattamento (cfr. sopra art. 7). Ciò significa anche che, a seconda delle modalità di comunicazione, in una legge dovrà essere prevista una base legale. I casi in cui si potrà derogare al requisito di una base legale sono disciplinati in modo esaustivo nel cpv. 2 e riprendono l'elenco delle eccezioni fissato dalla legge federale. In tale contesto è nuova in particolare la fattispecie d'eccezione quando il trattamento è necessario per

[1] La LADig è stata decisa dal Gran Consiglio il 16 ottobre 2023 ed entrerà in vigore presumibilmente il 1° aprile 2024.

proteggere la vita o l'integrità fisica della persona interessata o di un terzo (cfr. al riguardo l'art. 7).

Per ragioni di proporzionalità secondo il cpv. 4, quando si comunicano dati personali occorre sempre procedere con una ponderazione degli interessi. La comunicazione deve essere rifiutata, limitata o vincolata a condizioni se lo esigono importanti interessi pubblici o interessi manifestamente degni di protezione della persona interessata o se lo esige un obbligo legale di serbare il segreto o una disposizione speciale concernente la protezione dei dati. Come finora, su richiesta gli organi pubblici devono poter comunicare a terzi determinati dati di base. In diversi Cantoni questa eccezione è limitata agli organi pubblici preposti al controllo degli abitanti. Il Cantone dei Grigioni dispone di una disposizione analoga nell'art. 32 della legge sui registri degli abitanti e su altri registri delle persone e degli oggetti (LRAb; CSC 171.200). Dal momento che, stando ai rapporti di attività dell'incaricato della protezione dei dati[2], questa eccezione è stata invocata in diverse situazioni, deve essere mantenuta anche in questa sede. Con la comunicazione di dati di per sé oggettivamente innocui è possibile che, a seconda della fattispecie, vengano comunicate informazioni sensibili su una persona interessata. Anche per questo motivo, se vengono comunicati dati personali ai sensi del cpv. 3, anche in questo caso occorre procedere con una ponderazione degli interessi così come descritto nel cpv. 4. In conformità al diritto federale non sussistono più requisiti specifici per la comunicazione mediante procedure di richiamo (art. 19 cpv. 3 vLPD). Per procedure di richiamo si intendono procedure automatizzate che rendono possibile la comunicazione di dati personali a terzi tramite richiamo senza intervento da parte dell'organo pubblico che effettua la comunicazione. Nell'era digitale, questa specifica disposizione appare obsoleta. Anche nel caso di procedure di richiamo occorre tuttavia continuare a soddisfare i requisiti posti alla base legale. Se una procedura di richiamo (ad es. per via della modalità di trattamento di dati) comporta una grave ingerenza nei diritti fondamentali, è necessaria una base in una legge. Le disposizioni settoriali in materia di protezione dei dati che prevedono cosiddette procedure di richiamo possono invece essere mantenute e fungere da base legale per rispettive comunicazioni (cfr. ad es. l'art. 27a della legge sulla polizia del Cantone dei Grigioni [LPol; CSC 613.000]).

Art. 11 2. Comunicazione di dati personali nell'ambito dell'attività di informazione ufficiale

Attualmente la comunicazione di dati personali nel quadro dell'attività di informazione ufficiale si conforma all'art. 36 cpv. 3 e 5 LPD. L'articolo assume in ampia misura funzioni di coordinamento con la legge federale sulla trasparenza (LTras; RS 152.3). Per motivi di sistematica e chiarezza, nella LCPD la comunicazione di dati personali nel quadro dell'attività di informazione ufficiale sarà disciplinata in un articolo separato. Dal punto di vista giuridico-materiale vengono riprese le disposizioni vigenti se disciplinano d'ufficio l'informazione ufficiale del pubblico. Tale comunicazione è consentita se i dati sono in rapporto con l'adempimento di compiti pubblici e se sussiste un interesse pubblico preponderante alla comunicazione. Ai sensi del cpv. 2, i dati possono essere comunicati mediante servizi di informazione

[2] Cfr. ad es. il rapporto di attività 2013 dell'incaricato della protezione dei dati del Cantone dei Grigioni, pag. 11; rapporto di attività 2019 dell'incaricato della protezione dei dati del Cantone dei Grigioni, pag. 22.

e comunicazione automatizzati (ad es. internet o i social media) se una base legale lo prevede o se la comunicazione è ammessa conformemente al cpv. 1. I dati interessati dovranno essere cancellati non appena verrà meno l'interesse pubblico alla loro accessibilità.

Per quanto riguarda la protezione dei dati l'attività di informazione passiva (su richiesta) è disciplinata dall'art. 11 della legge sulla trasparenza, senza rimando alla LCPD. La disposizione contenuta in tale articolo disciplina in modo esaustivo l'evasione di relative domande e finora si è dimostrata valida. A differenza dell'art. 36 cpv. 3 LPD, si intende rinunciare anche in futuro a un rimando alla regolamentazione dell'attività di informazione passiva.

Art. 12 3. Comunicazione di dati personali all'estero

La comunicazione di dati personali all'estero presenta ulteriori rischi, non essendovi alcuna garanzia che nello Stato destinatario viga un livello di protezione dei dati equivalente. L'art. 12 disciplina pertanto la comunicazione di dati personali all'estero orientandosi agli art. 16 e 17 LPD. La comunicazione di dati all'estero è possibile soltanto se la legislazione dello Stato destinatario o l'organismo internazionale garantisce una protezione adeguata. A livello federale, la decisione in merito all'adeguatezza del livello di protezione dei dati spetta al Consiglio federale (art. 16 cpv. 1 LPD), che per dirimere la questione si attiene alle norme di diritto internazionale. Non vi è ragione per cui il Cantone dei Grigioni debba procedere secondo proprie valutazioni. Al contrario, appare sensato che il Cantone si attenga alle regole statuite dal Consiglio federale nelle disposizioni esecutive della LPD (FF 2017 6028). Di conseguenza, l'ordinanza relativa alla LCPD concernente la constatazione di un livello di protezione dei dati adeguato rimanderà al diritto federale.

Può accadere che la legislazione dell'altro Stato non garantisca un livello di protezione dei dati adeguato, ad esempio perché il Consiglio federale ha emesso una decisione negativa in tal senso. Da un lato, in tal caso i dati personali potranno essere comunicati all'estero soltanto se una protezione dei dati adeguata è garantita in un altro modo, ad esempio in forza di un trattato internazionale o di altre garanzie come le clausole contrattuali di protezione dei dati stipulate tra le parti. Dall'altro la comunicazione è ammessa, nei singoli casi, se sussistono i requisiti di cui all'art. 12 cpv. 2 lett. b-g (ad es. se la persona interessata ha espressamente acconsentito alla comunicazione). Dalla legge federale è stato ripreso anche il relativo elenco dei casi; eccezion fatta per qualche precisazione linguistica, tale elenco corrisponde alla situazione giuridica delineata dalla vLPD. Si tenga presente che la pubblicazione di dati personali nel quadro dell'attività di informazione ufficiale (cfr. sopra art. 11) non è considerata una comunicazione all'estero, neppure nel caso in cui i dati in questione siano accessibili dall'estero.

Art. 13 Trattamento di dati personali per scopi impersonali

L'art. 13 disciplina le condizioni in presenza delle quali si potrà agevolare il trattamento e la comunicazione di dati per scopi impersonali. La disposizione riprende in sostanza l'art. 39 LPD e non prevede alcuna novità rispetto al diritto previgente.

Art. 14 e art. 15 Sorveglianza con acquisizione di immagini dello spazio pubblico e pubblicamente accessibile

Con la revisione della LPol nel 2018, negli art. 3a e 3b LCPD sono state aggiunte norme che disciplinano la sorveglianza con acquisizione di immagini dello spazio pubblico. La decisione di inserire un'apposita norma all'interno della LCPD è motivata dall'intenzione di consentire anche ad altri organi pubblici, e non solo alla polizia, di avvalersi delle rispettive possibilità. Poiché, a quanto risulta, nella prassi le norme in materia si sono già dimostrate valide, non sussiste alcun bisogno di modificarle o di trasferirle in un'altra legge. Per questo motivo, nel quadro della revisione totale, gli art. 3a e 3b LCPD sono riprodotti con mere alterazioni di natura linguistica e i concetti verranno adeguati alla nuova terminologia (ad es. «organo pubblico» invece di «autorità»). In quanto lex specialis, la regolamentazione vigente relativa alla sorveglianza con acquisizione di immagini nei penitenziari (art. 23a legge sull'esecuzione giudiziaria nel Cantone dei Grigioni [LEG; CSC 350.500]) continua a prevalere sulla presente disposizione.

Art. 16 Archiviazione e distruzione

Attualmente le direttive relative all'archiviazione e alla distruzione di dati personali risultano dall'applicazione per analogia dell'art. 38 LPD, in virtù del rimando dinamico alla legge federale. Conformemente a questa disposizione, gli organi pubblici dovrebbero offrire all'Archivio di Stato i dati personali non più necessari. I dati che l'Archivio di Stato ha designato come non aventi valore archivistico devono essere distrutti, salvo che tali dati siano resi anonimi o debbano essere conservati a titolo di prova, per misura di sicurezza o per salvaguardare un interesse degno di protezione della persona interessata. Se applicata alla lettera, questa norma potrebbe creare incertezza giuridica. Da un lato, vi è il problema che nel Cantone non esiste un solo archivio, bensì, accanto all'Archivio di Stato, anche le regioni e i comuni gestiscono archivi propri che dispongono di competenze proprie (cfr. art. 12 LGAA). Dall'altro, la LGAA non riguarda le strutture sanitarie e le Chiese riconosciute dallo Stato, determinando di fatto la mancata applicabilità delle norme LCPD a queste strutture, le quali sono peraltro dotate di proprie norme di archiviazione. Il testo dell'art. 16 si discosta pertanto da quello della LPD federale, disponendo che i dati personali non più necessari debbano essere offerti all'archivio competente conformemente alle prescrizioni in vigore. Il cpv. 1 funge dunque da norma di coordinamento con le rispettive norme di archiviazione (ad es. nella LGAA). Il cpv. 2 disciplina la sorte dei dati personali che l'Archivio ha ritenuto non aventi valore archivistico e riprende la relativa norma vigente a livello federale. La prassi ha mostrato che vi è una grande incertezza per quanto riguarda i termini entro i quali i dati personali siano ancora ritenuti necessari. Per questo motivo, a titolo di novità il Governo dovrà poter emanare altre norme in materia di archiviazione e distruzione riguardanti, in modo particolare, i termini di cancellazione e le misure per la verifica regolare della necessità di insiemi di dati personali.

Art. 17 Obbligo di informare sulla raccolta di dati personali

L'art. 17 riprende in sostanza l'attuale art. 19 LPD. Come finora, la disposizione stabilisce che in linea di principio la persona interessata deve essere informata sulla raccolta di dati personali. Non vengono specificate le modalità con cui ciò debba avvenire. L'organo pubblico titolare del trattamento deve però garantire che la persona interessata possa effettivamente

prendere atto di queste informazioni. Il cpv. 2 disciplina le informazioni da comunicare. Alla persona interessata devono essere comunicate tutte le informazioni necessarie per consentirle di far valere i diritti che le spettano per legge e per garantire un trattamento trasparente dei dati. Oltre alle informazioni elencate nella legge federale, la persona interessata deve espressamente essere resa attenta ai suoi diritti (cfr. guida CdC, pag. 11).

Art. 18 Eccezioni all'obbligo di informare e limitazioni

L'art. 18 disciplina i casi in cui l'obbligo di informare può decadere o può essere limitato. La disposizione riprende in gran parte l'art. 20 LPD (nella misura in cui non riguarda soltanto titolari del trattamento privati). Per gli organi pubblici l'obbligo di informare può decadere se la persona interessata dispone già delle informazioni pertinenti. In molti casi il trattamento di dati da parte di organi pubblici non sarà associato a un obbligo di informare, in quanto il trattamento avviene in forza di una base legale che fornisce, in generale, informazioni relative ai dati oggetto di trattamento. Se i dati personali non sono raccolti presso la persona interessata, l'obbligo di informare può inoltre decadere se l'informazione non è possibile o richiede un onere sproporzionato. In conformità al diritto federale, questa disposizione d'eccezione deve essere interpretata in modo restrittivo.

In determinate circostanze, l'organo pubblico titolare del trattamento può inoltre limitare o differire l'informazione oppure rinunciarvi. A differenza del cpv. 1, in questi casi è necessario procedere a una ponderazione degli interessi. La limitazione, il differimento o la rinuncia sono giustificati soltanto nella misura in cui sussistano interessi contrapposti. I motivi soggiacenti alla suddetta limitazione sono analoghi ai motivi di restrizione del diritto d'accesso ai sensi dell’art. 25 LCPD (interessi preponderanti di terzi, interessi pubblici preponderanti, basi legali o rischio di compromettere un’indagine, un’istruzione o un procedimento giudiziario o amministrativo). Per ragioni di chiarezza, si rimanda pertanto a tale disposizione.

Art. 19 Valutazione d'impatto sulla protezione dei dati

L'art. 19 prevede che per determinati trattamenti di dati si effettui previamente una valutazione d'impatto sulla protezione dei dati. Questo obbligo è stato introdotto ex novo nel diritto federale con l'art. 22 LPD. Si tratta di uno strumento per individuare possibili rischi per le persone interessate già nelle fasi iniziali di un progetto e per poter così definire provvedimenti atti a far fronte a tali rischi. In questo modo si potrà garantire una migliore protezione dei dati, evitando di dover eventualmente intervenire in un secondo momento con costosi interventi correttivi. La valutazione d'impatto sulla protezione dei dati deve essere effettuata ogni qualvolta il trattamento di dati previsto (sulla base di una stima preliminare da parte dell'organo pubblico titolare del trattamento) possa comportare un rischio elevato per i diritti fondamentali della persona interessata. Le situazioni in cui il rischio è elevato dovranno essere disciplinate a livello di ordinanza (come nella maggior parte dei Cantoni). Per la definizione si farà riferimento alla legge federale, secondo la quale un rischio elevato sussiste in particolare in caso di utilizzazione di nuove tecnologie o di un trattamento su grande scala di dati personali degni di particolare protezione. L'art. 19 disciplina i contenuti minimi della valutazione d'impatto sulla protezione dei dati in conformità al diritto federale. Il fatto di doversi occupare di aspetti inerenti la protezione dei dati non è del tutto nuovo, almeno non per le autorità

dell'Amministrazione cantonale. In base alla direttiva «IKT-Sicherheit in der Kantonalen Verwaltung Graubünden» (Sicurezza TIC nell'Amministrazione cantonale dei Grigioni), i servizi e i Dipartimenti devono effettuare un'analisi della necessità di protezione ogni qualvolta introducono nuovi trattamenti di dati. Se la necessità di protezione risulta elevata, occorre elaborare un piano per la sicurezza dell'informazione e la protezione dei dati in collaborazione con l'incaricato della sicurezza dell'informazione. Tale piano contiene nello specifico un'analisi dei rischi ed eventuali provvedimenti di sicurezza aggiuntivi o rischi residui. Si può utilizzare questo documento come base per effettuare la valutazione d'impatto sulla protezione dei dati.

Art. 20 Consultazione preliminare

Secondo il diritto internazionale, determinati progetti che prevedono il trattamento di dati devono essere preliminarmente sottoposti all'organo di vigilanza per una consultazione preliminare. Tale consultazione preliminare viene considerata un mezzo efficace ai fini della protezione preventiva dei dati. L'obbligo di consultazione preliminare è sancito soltanto dalla direttiva 2016/680 e potrebbe trovare applicazione esclusivamente nell'ambito della cooperazione giudiziaria e di polizia. Ciononostante, a quanto risulta tutti i Cantoni hanno deciso di introdurre lo strumento della consultazione preventiva per l'intero diritto amministrativo cantonale. Questo strumento deve quindi essere introdotto anche nel Cantone dei Grigioni. La consultazione preliminare dovrà essere eseguita ogni qualvolta che, nonostante i provvedimenti previsti dall'organo pubblico titolare del trattamento, il trattamento di dati previsto comporta un rischio elevato per i diritti fondamentali della persona interessata. L'obiettivo della consultazione preliminare è garantire che l'organo di vigilanza possa occuparsi sin dal principio della problematica legata alla protezione dei dati in un determinato progetto. A livello federale, la consultazione preliminare è prevista nell'art. 23 LPD, disposizione che viene quindi ripresa in ampia misura. Fissare a livello di legge un termine di elaborazione come avviene nella legge federale non è ritenuto opportuno. La consultazione preliminare può senz'altro avvenire più rapidamente se di piccola entità, mentre in progetti più complessi ha comunque luogo in maniera scaglionata in base alle fasi del progetto. L'elaborazione da parte dell'organo di vigilanza deve quindi avvenire «entro un termine adeguato», ma l'incaricato deve comunque orientarsi al termine di due mesi statuito dalla Confederazione e da altri Cantoni.

Art. 21 Notifica di violazioni della sicurezza dei dati

A seguito delle disposizioni del diritto internazionale, con la revisione nella legge federale è stato introdotto l'obbligo di notificare violazioni della sicurezza dei dati (art. 24 LPD). Questa disposizione sarà ripresa nell'art. 21. L'organo pubblico titolare del trattamento deve notificare quanto prima all'organo di vigilanza ogni violazione della sicurezza dei dati che comporta verosimilmente un rischio elevato per i diritti fondamentali della persona interessata. È considerata violazione della sicurezza dei dati qualsiasi violazione della sicurezza in seguito alla quale, in modo accidentale o illecito, dati personali vengono persi, cancellati, distrutti, modificati oppure divulgati o resi accessibili a persone non autorizzate (cfr. art. 3 cpv. 8). Dalla legge federale vengono ripresi anche il testo concernente l'obbligo di notifica e l'ulteriore procedura (ad es. quando è necessaria la notifica alla persona interessata). In determinate circostanze possono essere previste limitazioni all'obbligo di notifica di violazioni della sicurezza dei dati. Per una maggiore chiarezza, a differenza della legge federale si rinuncia

in questo caso a un rimando ad altre disposizioni. Rimangono tuttavia invariati i motivi di esclusione (in particolare interessi pubblici preponderanti, impossibilità di informare, obblighi vigenti di serbare il segreto).

Art. 22 Registro delle attività di trattamento

Secondo il diritto vigente, l'organo di vigilanza è obbligato a tenere un registro pubblico delle collezioni di dati che gli devono essere notificate dalle autorità soggette alla legge (art. 4 cpv. 1 LCPD). Considerato che sinora questo registro è stato gestito e aggiornato in maniera molto rudimentale, il valore informativo di questo registro è scarso. Inoltre, i diritti delle persone interessate possono essere salvaguardati anche senza registro, motivo per cui l'obbligo di tenere tale registro appare obsoleto e viene dunque stralciato. La direttiva 2016/680 prevede invece un obbligo di tenere un registro delle attività di trattamento dei dati. In base al campo di applicazione della direttiva 2016/680, è sufficiente che tale registro venga redatto nell'ambito del trattamento di dati da parte degli organi giudiziari e di polizia. A differenza della Confederazione (art. 12 LPD), il Cantone dei Grigioni non imporrà quindi quest'obbligo a tutti gli organi pubblici soggetti alla legge. Dovrà spettare al Governo designare, nel quadro dell'ordinanza, gli organi pubblici soggetti alla tenuta del registro (segnatamente le autorità preposte all'esecuzione giudiziaria e al perseguimento penale). Soltanto per quanto riguarda i tribunali penali (conformemente alla legge d'applicazione del Codice di diritto processuale penale svizzero [LACPP; CSC 350.100]) non sarà sufficiente una norma a livello di ordinanza. I tribunali penali devono quindi essere indicati nella legge. Per altre autorità amministrative cantonali e in particolare per i comuni non sussisterà l'obbligo di tenere un registro delle attività di trattamento. Tuttavia, dal momento che il registro può rappresentare una fonte importante per dimostrare il rispetto delle disposizioni sulla protezione dei dati come richiesto in futuro ai sensi dell'art. 4 cpv. 2 LCPD, tutti gli organi pubblici soggetti alla LCPD potranno scegliere liberamente di tenere questo registro. Ai cpv. 2 e 3 sono disciplinati i contenuti richiesti in base all'art. 12 LPD. L'organo pubblico titolare del trattamento è tenuto a notificare il registro all'organo di vigilanza e ad aggiornarlo costantemente.

Art. 23 Consulente per la protezione dei dati

Ai sensi della direttiva 2016/680, le autorità preposte al trattamento di dati giudiziari e di polizia sono tenute a nominare una persona responsabile della consulenza in materia di protezione dei dati (consulente per la protezione dei dati). A livello federale, questo strumento è disciplinato nell'art. 10 LPD e deve presumibilmente essere previsto per tutti gli organi federali (cfr. art. 27 OLPD). Il consulente per la protezione dei dati ha il compito di fornire consulenza e supporto al personale per questioni inerenti al trattamento di dati personali, assicurando che il titolare del trattamento effettui la valutazione d'impatto sulla protezione dei dati (cfr. art. 19 LCPD) e fungendo da interlocutore per l'organo di vigilanza. Per ora soltanto la Polizia cantonale si avvale di un incaricato della protezione dei dati ai sensi dell'art. 43 cpv. 3 dell'ordinanza sulla polizia (OPol; CSC 613.100). In base al campo d'applicazione della direttiva 2016/680, questo obbligo sarà invece esteso ad altre autorità. Così come per il registro delle attività di trattamento, l'obbligo per i tribunali penali e le altre autorità soggette alla direttiva 2016/680 deve essere disciplinato nella LCPD e precisato nell'ordinanza di esecuzione. Ma anche altre autorità possono designare una persona responsabile della consulenza per

la protezione dei dati.

Art. 24 Diritto d'accesso

Il diritto di una persona a essere informata riguardo all'eventualità di trattamento dei suoi dati e, se del caso, a quali dati vengono trattati da un organo pubblico rappresenta uno dei punti centrali del diritto sulla protezione dei dati nonché il punto di partenza per far valere altri diritti e pretese spettanti alla persona interessata. Il diritto d'accesso è già garantito dalla legge vigente in virtù dell'art. 5 cpv. 1 LCPD; a seguito del rimando dinamico la disposizione viene concretizzata dall'art. 25 LPD. Anche la regolamentazione nell'art. 24 continuerà a orientarsi a quella nella LPD. Rispetto al diritto federale precedente, il diritto d'accesso è stato concretizzato nel senso che ora devono essere comunicate tutte le informazioni necessarie per far valere i diritti sanciti dalla legge in oggetto e per garantire un trattamento trasparente dei dati. Segnatamente, alla persona devono essere fornite le informazioni che devono essere comunicate anche nel quadro dell'obbligo di informare di cui all'art. 17 cpv. 2. In questa sede si può pertanto rimandare alla relativa disposizione. In conformità alla legge federale, vige inoltre l'obbligo di comunicare la durata di conservazione e la provenienza dei dati personali.

Art. 25 Restrizione del diritto d'accesso

Come finora (cfr. art. 5 cpv. 1 LCPD in unione con l'art. 26 LPD), il diritto d'accesso deve poter essere assoggettato a restrizioni. Le ragioni legittimanti una restrizione sono state in gran parte riprese dalla vecchia legge federale. L'informazione può quindi rimanere limitata se e nella misura in cui lo preveda un obbligo legale particolare di serbare il segreto o lo esigano un interesse pubblico preponderante o interessi preponderanti di terzi (ad es. per proteggere altre persone interessate), oppure qualora la fornitura delle informazioni rischi di compromettere un'indagine, un'istruzione o un procedimento giudiziario o amministrativo. Dalla legge federale non sarà ripresa la possibilità di limitare l'informazione se la domanda d'accesso è manifestamente infondata o dovuta a una condotta querulomane. Secondo le disposizioni del diritto internazionale, questa regolamentazione non deve essere necessariamente ripresa (essa è anzi addirittura giudicata incompatibile con la Convenzione SEV 108, cfr. FF 2017 5939, 6057). Essa rappresenterebbe peraltro un indebolimento dei diritti delle persone interessate.

Art. 26 Opposizione alla comunicazione di dati personali

In determinate circostanze, la persona interessata deve poter vietare all'organo pubblico la comunicazione di dati personali. Questo diritto della persona interessata era già previsto dalla precedente legge e denominato «blocco» (art. 20 vLPD). In linea con il diritto europeo, nell'art. 37 LPD si parla ora di opposizione alla comunicazione. I materiali partono comunque dal presupposto che il contenuto materiale della disposizione non cambierà (cfr. FF 2017, 6070). Ciò significa che l'opposizione è possibile in qualsiasi momento e non soltanto in relazione a una specifica comunicazione. La persona interessata deve far valere un interesse degno di protezione all'opposizione alla comunicazione (ad es. la prevenzione di possibili molestie o vessazioni). La domanda di opposizione potrà essere respinta o non considerata qualora sussista un obbligo legale di comunicazione o qualora l'adempimento del compito dell'organo pubblico ne risulti pregiudicato. Siccome di solito la comunicazione di dati tra organi pubblici avviene in virtù di una base legale (cfr. art. 9 LCPD), il diritto di opposizione si

applica principalmente alla comunicazione di dati a privati o ad autorità straniere. Dall'art. 10 cpv. 2 lett. d LCPD risulta inoltre che un'opposizione può essere respinta anche nel caso in cui il destinatario sia in grado di dimostrare che la persona richiedente si sia avvalsa del diritto di opposizione in maniera abusiva (ad es. per impedire l'attuazione di pretese giuridiche).

Art. 27 Altre pretese

La LCPD deve offrire alle persone interessate la possibilità di difendersi dal trattamento illecito (ad es. in assenza di una base legale sufficiente) dei loro dati. A tale scopo, la persona interessata può far valere diversi diritti disciplinati nell'art. 27 LCPD, tra cui il diritto all'astensione dal trattamento illecito, all'eliminazione delle conseguenze di un trattamento illecito e all'accertamento del carattere illecito del trattamento, nonché il diritto di rettifica di dati inesatti. Tali diritti sono già previsti dal diritto vigente nell'art. 5 LCPD in unione con l'art. 41 LPD. Nell'art. 41 cpv. 3 LPD la legge federale prevede la limitazione del trattamento quale alternativa meno incisiva rispetto alla cancellazione, disponendo che, nei casi indicati dalla legge, sia ammesso l'ulteriore trattamento dei dati, ma solo a determinati scopi. Trattandosi di uno strumento che nessun altro Cantone ha adottato, si rinuncia alla sua introduzione anche in questa sede. Come finora, se non possono essere accertate né l'esattezza né l'inesattezza dei dati personali in questione, l'organo pubblico può aggiungere una menzione che indichi il carattere contestato anziché la rettifica di un dato personale. Non viene invece ripresa dalla legge federale la norma concernente i fondi delle istituzioni pubbliche della memoria collettiva (ad es. archivi e musei). Se a essere interessati sono gli archivi, in virtù dell'art. 2 cpv. 4 LCPD prevalgono le norme speciali previste dalla LGAA. In deroga al diritto federale, nell'art. 11 cpv. 1 LGAA tali norme prevedono, anch'esse, la possibilità di apporre una menzione che indichi il carattere contestato, ragione per cui non sussiste motivo per riprendere questa disposizione. Per quanto riguarda altre istituzioni della memoria collettiva sarebbe eventualmente ipotizzabile una norma separata. Tuttavia, a quanto risulta, nessun altro Cantone ha emanato una norma in tal senso e quindi vi si può rinunciare anche nel Cantone dei Grigioni.

Art. 28 Procedura

Le persone interessate devono poter adire le vie legali in caso di violazione dei diritti loro riconosciuti dalla presente legge. Pertanto, l'organo pubblico è tenuto a motivare la propria decisione se respinge una richiesta ai sensi della presente legge. Nella legge in vigore, questa fattispecie è disciplinata nell'art. 6. La disposizione non risulta convincente sotto vari aspetti e deve essere rivista. I cpv. 1 e 3 dell'art. 6 LCPD non si scostano dalla regolamentazione delle competenze ancorata nella LGA (cfr. art. 28 LGA) e risultano pertanto superflui. L'art. 6 cpv. 2 LCPD attualmente in vigore prevede che, contro le decisioni di privati che assolvono compiti pubblici, sia aperta la via del ricorso all'autorità mandataria. La delega di un compito pubblico è associata alla facoltà di emanare decisioni se tale possibilità è espressamente prevista o se la possibilità di emanare decisioni risulta necessaria all'adempimento del compito pubblico oggetto della delega. Se il soggetto privato incaricato è autorizzato a emanare disposizioni, il diritto di ricorso deve essere allora disciplinato nella normativa di settore. In tal senso, anche il diritto di ricorso sinora previsto dall'art. 6 cpv. 2 può essere stralciato perché

superfluo. Un’altra disposizione che ha trovato scarsa adesione negli altri Cantoni è quella dell'art. 6 cpv. 4, secondo cui l'organo di vigilanza dispone di un diritto di ricorso contro le decisioni di un organo pubblico rivolte a un privato (concernenti il riconoscimento di diritti delle persone interessate). In virtù del diritto internazionale è sufficiente consentire all'organo di vigilanza di emanare disposizioni vincolanti concernenti la violazione del diritto sulla protezione dei dati nei confronti di organi pubblici, che le possono poi a loro volta impugnare in sede giudiziaria. È una competenza che l'organo di vigilanza acquisisce ora insieme alla competenza di emanare decisioni ai sensi dell'art. 37 LCPD. Non c'è necessità di concedere all'organo di vigilanza un ulteriore diritto di ricorso.

In base alle disposizioni di diritto internazionale, il diritto d'accesso quale strumento più importante per le persone interessate e quale punto di partenza per far valere altri diritti dovrebbe in linea di principio essere concesso gratuitamente. Lo stesso vale per le richieste di rettifica di dati personali inesatti. Anche la richiesta di blocco dei dati personali dovrebbe essere concessa gratuitamente, perché, per quanto meno rilevante sul piano pratico, è risaputo per esperienza che richiede un onere modesto. Il Governo deve però poter derogare a questo principio, segnatamente se una richiesta comporta un onere sproporzionato. Tendenzialmente, invece, la valutazione delle altre pretese in materia di protezione dei dati è più onerosa. Per questo motivo (in linea con quanto disposto in gran parte dei Cantoni) per tali altre pretese si rinuncia all'esenzione dalle spese. In tali casi la riscossione degli emolumenti si conforma ai principi generali. Per il resto, la procedura si conforma alla LGA.

Art. 29 Procedura in caso di comunicazione di documenti ufficiali che contengono dati personali

Già secondo il diritto in vigore, nelle procedure previste dalla legge sulla trasparenza la persona interessata può non soltanto chiedere che i dati personali in questione non vengano comunicati, bensì può anche far valere gli altri diritti che le spettano (cfr. art. 5 LCPD in unione con l'art. 42 LPD). Questa possibilità serve a coordinare le procedure previste dalla legge sulla protezione dei dati e dalla legge sulla trasparenza; essa verrà pertanto mantenuta.

Art. 30 Organo di vigilanza

Il diritto internazionale dispone che un organo di controllo indipendente vigili sul trattamento di dati da parte delle autorità e sull'applicazione delle disposizioni sulla protezione dei dati. A tal fine, sin dall'entrata in vigore della LCPD il Cantone dei Grigioni si avvale di un incaricato della protezione dei dati che funge da organo di vigilanza. Quest'organo di vigilanza deve essere mantenuto. Tenuto conto del campo di applicazione, i trattamenti di dati nei procedimenti giudiziari e nei procedimenti secondo gli ordinamenti procedurali federali nonché nelle procedure di giurisdizione amministrativa dovranno essere esclusi dal controllo dell'organo di vigilanza (art. 2). Come previsto dal diritto europeo, i tribunali saranno tuttavia soggetti al controllo dell'organo di vigilanza per quanto concerne altri trattamenti di dati (cfr. art. 15 n.10 Convenzione STE 108).

Art. 31 Statuto

Per poter svolgere in maniera efficace la sua funzione di vigilanza, l'organo di vigilanza deve essere autonomo e indipendente sotto il profilo professionale e non essere vincolato alle direttive di altri organi nell'adempimento dei suoi compiti, né in termini di contenuti né in termini di contenuti né in termini di entità (cfr. già secondo il diritto in vigore art. 7 LCPD). Ciononostante deve essere ammessa una certa vigilanza gerarchica che, in virtù del diritto internazionale, deve orientarsi alla vigilanza organica che esiste ad esempio per i tribunali. Questa funzione di vigilanza viene assunta dal Governo in quanto organo di elezione. In questa funzione il Governo deve tenere conto dell'indipendenza dell'organo di vigilanza. In particolare, in caso di grave violazione dei doveri d'ufficio o di incapacità permanente di esercitare la carica, il Governo deve però avere la facoltà di destituire l'incaricato della protezione dei dati e il suo supplente (cfr. art. 32 subito sotto). Come finora, sul piano amministrativo, l'organo di vigilanza è subordinato alla Cancelleria dello Stato. Per «subordinazione amministrativa» (cfr. art. 16 legge sull'organizzazione del Governo e dell'Amministrazione [LCOGA; CSC 170.300]) s'intende semplicemente che la Cancelleria dello Stato assiste l'organo di vigilanza nell'adempimento dei compiti che gli sono stati delegati (ad es. attraverso la messa a disposizione di infrastrutture). La subordinazione alla Cancelleria dello Stato in quanto organo di coordinamento e di collegamento tra il Parlamento, il Governo e l'Amministrazione viene praticata in diversi altri Cantoni e ritenuta come un vantaggio. Pertanto deve essere mantenuta.

Poiché l'organo di vigilanza costituisce un'unità amministrativa dell'Amministrazione cantonale (cfr. sopra art. 30), a tale organo si applica in linea di principio il diritto cantonale sul personale e sulla Cassa pensioni. Dalle disposizioni di diritto internazionale concernenti l'indipendenza dell'organo di vigilanza risultano alcuni aspetti del diritto sul personale e sulla Cassa pensioni che non possono tuttavia essere applicati senza ulteriori precisazioni e che quindi vengono disciplinati in maniera diversa nella presente legge. Si tratta segnatamente dell'indipendenza da direttive, della procedura di nomina e della destituzione dalla carica (art. 32). Risulta invece sensato non applicare, per l'incaricato della protezione dei dati e per il suo supplente, lo scatto per anzianità previsto dalla legge sul personale, bensì attribuirli direttamente al livello massimo di una classe di funzione.

Art. 32 Nomina

Secondo il diritto internazionale, gli incaricati della protezione dei dati devono essere nominati dal Parlamento, dal Governo o da un organo indipendente tramite una procedura di nomina trasparente. Attualmente nel Cantone dei Grigioni l'incaricato della protezione dei dati viene nominato a tempo indeterminato dal Governo e assunto con un rapporto di mandato revocabile in qualsiasi momento (cfr. art. 7 LCPD). La nomina da parte del Governo si è dimostrata valida e deve essere mantenuta. L'aspetto ritenuto problematico sotto il profilo dell'indipendenza riguarda invece la revocabilità, in qualsiasi momento, del rapporto di mandato. In futuro, l'incaricato della protezione dei dati dovrà quindi essere nominato per un mandato di quattro anni, così come è prassi per la maggior parte delle cariche pubbliche nel Cantone dei Grigioni e in numerosi altri Cantoni, con possibilità di riconferma. La possibilità di destituzione dal mandato in caso di incapacità permanente di esercitare la carica o in caso

di grave violazione intenzionale o per negligenza dei doveri d'ufficio è compatibile con le prescrizioni del diritto internazionale.

Poiché con l'attuale grado di occupazione del 50% l'incaricato della protezione dei dati non sarà in grado di far fronte ai compiti attuali e futuri, è previsto che nell'organo di vigilanza vi sia almeno un'altra persona che assuma anche compiti di supplenza (cfr. capitolo V). Oltre a una persona con formazione giuridica, vengono richieste anche conoscenze approfondite di informatica, poiché soltanto così potrà essere garantito un adempimento sensato di determinati compiti (ad es. la valutazione di casi di violazione della sicurezza dei dati). Sinora l'incaricato della protezione dei dati ricorreva a consulenti esterni per acquisire le conoscenze specialistiche necessarie, offrendo una ricompensa dall'importo forfettario riconosciuto alla sua funzione. Di conseguenza, risulta più opportuno creare competenze interne all'organo cantonale. Nel caso ideale, grazie alle sue competenze il supplente deve completare la direzione (ad es. uno specialista IT se l'incaricato è un esperto in giurisprudenza e viceversa). Si ritiene opportuno applicare al supplente le stesse regole valide per l'incaricato della protezione dei dati per quanto attiene alla nomina e alla destituzione dal mandato.

Art. 33 Incompatibilità

L'indipendenza dell'incaricato della protezione dei dati può essere compromessa anche dall'esercizio di attività accessorie. Attualmente la LCPD non contiene disposizioni in materia. In conformità alle norme internazionali, all'incaricato della protezione dei dati è vietato ricoprire un'altra carica pubblica. L'obiettivo è evitare che nella sua funzione l'incaricato della protezione dei dati si ritrovi a controllare un organo pubblico cui esso stesso appartiene. In considerazione della sfera d'azione dell'incaricato della protezione dei dati, altri Cantoni valutano come importante anche l'imparzialità politico-partitica. In tal senso, la limitazione riguarderà soltanto il divieto per l'incaricato della protezione dei dati di assumere una funzione direttiva in seno a un partito politico. Se l'incaricato della protezione dei dati ricopre questa funzione a tempo pieno, in linea di principio un'altra attività lucrativa è esclusa. Se l'incaricato della protezione dei dati ricopre la sua funzione come finora a tempo parziale, si pone la domanda se e a quali condizioni gli debba essere concesso il diritto di esercitare un'attività accessoria. Dal diritto internazionale non si può derivare un divieto rigoroso di attività accessorie. Come in altri Cantoni, l'esercizio di un'altra attività lucrativa deve essere ammessa se l'incaricato della protezione dei dati svolge la sua attività a tempo parziale. Tuttavia, questa attività deve essere autorizzata da parte del Governo in quanto organo di nomina. Conformemente al diritto internazionale, l'autorizzazione di esercitare un'altra attività lucrativa potrà essere negata soltanto qualora tale seconda attività pregiudichi l'esercizio della funzione nonché l'indipendenza e la reputazione di quest'organo (cfr. art. 42 cpv. 3 direttiva 2016/680). Le stesse regole si applicano anche al supplente dell'incaricato della protezione dei dati.

Art. 34 Preventivo

L'organo di vigilanza può adempiere i suoi compiti previsti dalla legge in modo completamente indipendente soltanto se riceve le risorse necessarie e può disporne liberamente. Attualmente l'incaricato della protezione dei dati è assunto con un contratto di diritto privato che può essere risolto in qualsiasi momento. Le risorse finanziarie attualmente erogate a favore dell'incaricato della protezione dei dati sono definite dalla struttura stessa dell'incarico e sono

assegnate al preventivo della Cancelleria dello Stato. In base alle cifre riportate nel conto annuale, si tratta di un contributo fisso concordato e costante nel tempo. Con i nuovi compiti e obblighi derivanti dalla revisione, l'importo precedentemente concordato difficilmente basterà a coprire i costi per un adempimento efficace dei compiti. Sebbene l'organo di vigilanza sia in linea di principio libero nell'impiego dei fondi sinora stanziati, per ragioni di indipendenza (come in altri Cantoni) in futuro deve essere permesso l'allestimento di un proprio preventivo. Al fine di rafforzare l'indipendenza dal Governo in quanto organo di nomina, è previsto che in linea di principio il Governo inserisca il progetto di preventivo senza modifiche nel suo preventivo all'attenzione del Gran Consiglio (nel Cantone si procede in maniera analgoa anche nel caso del Controllo delle finanze, cfr. art. 6 legge sulla vigilanza finanziaria [LVF; CSC 710.300]). Il Governo è naturalmente libero di proporre modifiche al Gran Consiglio. La decisione in merito al preventivo richiesto spetta al Gran Consiglio. L'incaricato della protezione dei dati può disporre liberamente, sotto la propria responsabilità, del preventivo approvato dal Parlamento per l'impiego di personale e l'utilizzo dei fondi.

Art. 35 Compiti

L'art. 35 disciplina i compiti dell'organo di vigilanza. Questi compiti sono già previsti dalla legge attuale nell'art. 8 e devono essere ripresi in ampia misura. In virtù delle disposizioni del diritto internazionale e dei nuovi strumenti vi si aggiungono tuttavia nuovi ambiti. A titolo di novità, nella legge viene perciò stabilito che l'organo di vigilanza deve svolgere anche attività di sensibilizzazione nei confronti degli organi pubblici e che deve seguire gli sviluppi determinanti nel settore delle tecnologie dell'informazione e della comunicazione. Viene sottolineata espressamente anche la cooperazione con altri organi pubblici. Non è invece più previsto che l'organo di vigilanza tenga un registro delle attività di trattamento dei dati (cfr. sopra art. 22). Le disposizioni del diritto internazionale prevedono inoltre il diritto per le persone interessate di poter proporre ricorso dinanzi all'organo di vigilanza indipendentemente da altri rimedi offerti dal diritto amministrativo o giudiziario. È considerato sufficiente se le direttive legislative prevedono che la persona interessata ha la possibilità di notificare all'organo di vigilanza qualsiasi inosservanza delle prescrizioni sulla protezione dei dati nell'elaborazione dei propri dati personali. Questa possibilità deve essere tuttavia resa disponibile indipendentemente da altri rimedi di diritto amministrativo o giudiziario (distinguendosi in questo, ad es., dal ricorso di vigilanza di cui all'art. 68 LGA). L'organo di vigilanza è tenuto a occuparsi di questa istanza e può, su tale base, adottare ulteriori misure (cfr. art. 36 e 37). La persona interessata non ha diritti di parte, ma essa deve essere informata entro tre mesi in merito all'esito o allo stato degli accertamenti.

Art. 36 e 37 Competenze

L'organo di vigilanza necessita di ampie competenze per l'adempimento dei propri compiti. Già secondo il diritto vigente (cfr. art. 9 e 10 LCPD) è autorizzato a richiedere agli organi pubblici, per via scritta e orale, informazioni concernenti il trattamento di dati personali, a visionare collezioni di dati e la rispettiva documentazione e a esigere che gli sia esibito il trattamento di dati personali. Gli organi pubblici sono tenuti ad assistere l'organo di vigilanza nell'adempimento dei suoi compiti. Le competenze di cui già dispone saranno mantenuti,

seppur con alcuni aggiustamenti terminologici. Attualmente, l'organo di vigilanza può sollecitare, ma unicamente ai sensi di una raccomandazione, un organo pubblico ad adottare le misure necessarie se emerge che quest'ultimo ha violato prescrizioni in materia di protezione dei dati. Se l'organo pubblico non dà seguito a questa raccomandazione o la rifiuta, l'organo di vigilanza deferisce la pratica al Governo. In futuro l'organo di vigilanza deve poter ancora formulare raccomandazioni corrispondenti. Per rafforzare lo statuto dell'organo di vigilanza, a titolo di novità, in virtù del diritto internazionale, quest'ultimo dovrà avere in aggiunta anche la competenza di emanare disposizioni vincolanti (sotto forma di decisione) in caso di violazione del diritto sulla protezione dei dati. L'organo di vigilanza dovrebbe poter ricorrere a questa possibilità in «ultima ratio» nel caso in cui un organo non dia seguito alla raccomandazione o invii chiari segnali in tal senso. In base al diritto internazionale, all'organo di vigilanza deve essere conferita la facoltà di adottare provvedimenti cautelari in presenza di rischi evidenti o di violazione di interessi degni di protezione. Questa competenza è stata già conferita dall'art. 5 LGA e non vi è dunque necessità di ancorarla espressamente nella LCPD. Le decisioni dell'organo di vigilanza possono essere impugnate dinanzi al Tribunale d'appello[3]. Dal momento che il Tribunale d'appello stesso potrebbe essere destinatario delle decisioni dell'organo di vigilanza (cfr. l'eccezione relativa ai trattamenti di dati nei procedimenti giudiziari in corso, art. 30 cpv. 2), è poco sensato accordare allo stesso la facoltà di pronunciarsi in merito a tali decisioni in veste di autorità di ricorso. Pertanto, le decisioni dell'organo di vigilanza riguardanti il Tribunale d'appello devono essere delegate alla competenza del Tribunale di giustizia (cfr. art. 63 e segg. LGA).

Art. 38 Rapporto

Già secondo il diritto vigente, l'incaricato della protezione dei dati deve presentare al Governo un rapporto sulla propria attività. Nel quadro della presente revisione si specifica l'oggetto di questo obbligo di presentare rapporto. Inoltre, se un organo pubblico è destinatario di una raccomandazione o di una decisione dell'organo di vigilanza, a titolo di novità deve essere invitato a prendere posizione prima della pubblicazione del rapporto. Nella sua presa di posizione l'organo pubblico può specificare in particolare i provvedimenti previsti, avviati o già adottati. La presa di posizione dell'organo pubblico deve essere allegata al rapporto. Come in precedenza, il rapporto dell'organo di vigilanza deve essere pubblicato.

Art. 39 Discrezione

In virtù delle sue competenze di controllo (cfr. art. 36 LCPD), l'organo di vigilanza dispone di ampi diritti di presa in visione. A esso non possono essere contrapposte nemmeno disposizioni particolari relative all'obbligo di serbare il segreto. Per tutelare il segreto, l'organo di vigilanza è soggetto agli stessi obblighi di discrezione previsti per l'organo pubblico che tratta i dati. Questo obbligo di discrezione è già sancito dalla legge attualmente in vigore nell'art. 10 LCPD e viene ripreso in gran parte senza modifiche. Viene tuttavia chiarito che l'obbligo di

[3] Nel quadro della riforma della giustizia 3, con effetto al 1° gennaio 2025 il Tribunale amministrativo cantonale competente in materia verrà accorpato al Tribunale cantonale andando a costituire un unico Tribunale d'appello. In seno al Tribunale d'appello, la competenza per le pratiche in questione spetterà alla sezione incaricata dell'evasione delle pratiche di diritto amministrativo.

discrezione non termina con l'abbandono della carica, bensì rimane applicabile anche in seguito.

Art. 40 Disposizioni penali

Finora, conformemente all'art. 10a cpv. 1 LCPD, viene punito a querela di parte con una multa «chi quale persona impiegata o incaricata di un'autorità o quale persona impiegata da una persona incaricata viola intenzionalmente le disposizioni del diritto cantonale sulla protezione dei dati». Questa formulazione potrebbe tuttavia contravvenire al principio di legalità, dal momento che per le persone interessate risulta difficile intuire quale sia il comportamento passibile di punizione. Per questo motivo sono state adeguate anche le disposizioni penali. La legge attuale consente già ora di punire efficacemente numerosi casi di violazione della protezione dei dati con applicazione di sanzioni di diritto penale e di diritto del personale per violazioni del segreto d'ufficio o professionale. Le possibilità sanzionatorie previste dal diritto vigente sono però troppo deboli per poter essere applicate anche ai dati personali che esulano dalle aree specifiche del diritto penale e del diritto del personale. È il caso, in particolare, della comunicazione di dati personali in relazione all'outsourcing e al trattamento di dati per scopi impersonali. In conformità alle leggi sulla protezione dei dati vigenti in altri Cantoni, in futuro comportamenti chiaramente definiti in queste aree potranno essere espressamente puniti con la multa. Il procedimento penale si conforma in questo caso alle norme del Codice di diritto processuale penale svizzero (CPP; RS 312.0).

Art. 41 Disposizioni transitorie 1. Disposizione transitoria relativa ai trattamenti in corso

Gli organi pubblici sono tenuti ad adeguare i propri trattamenti di dati al nuovo diritto. Da un lato ciò interessa alcuni tipi di trattamento di dati per i quali, a titolo di novità, sono previsti requisiti più severi (ad es. per i dati ora da classificare come dati personali degni di particolare protezione o eventualmente come profilazione). Dall'altro, tutti gli organi pubblici titolari del trattamento dovranno conformarsi a determinati nuovi obblighi e strumenti (ad. es. la valutazione d'impatto sulla protezione dei dati o la notifica di violazioni della sicurezza dei dati). Nel quadro della revisione non si è proceduto a una verifica sistematica riguardo al fatto se in questi casi le basi legislative contenute nelle leggi speciali siano sufficientemente precise e il loro livello normativo sia adeguato per soddisfare i requisiti posti a una base legale per il trattamento o la comunicazione di dati personali. Questa verifica deve essere effettuata per ogni singolo settore. Nella misura in cui gli organi pubblici si attengono alle direttive vigenti, la necessità di adeguamento è classificabile come moderata. Ciononostante è incontestato che l'adeguamento al nuovo diritto richiederà del tempo. Per questo motivo, agli organi pubblici deve essere concesso un periodo transitorio di due anni. Al più tardi dopo la scadenza di questo termine, i trattamenti di dati avviati e portati avanti lecitamente ai sensi del diritto previgente dovranno soddisfare i requisiti della LCPD. Ciò significa, da un lato, che i trattamenti in questione sono ammessi in virtù delle basi legali esistenti nella rispettiva legge speciale. Dall'altro, gli strumenti e gli obblighi ancorati nella legge dovranno essere attuati soltanto dopo un periodo transitorio di due anni.

Art. 42 2. Prima nomina dell'incaricato della protezione dei dati

In futuro l'incaricato della protezione dei dati non sarà più nominato una sola volta, bensì per un mandato di quattro anni. A causa del cambio di sistema, la prima nomina deve essere disciplinata nel quadro di una disposizione transitoria. La prima nomina avrà effetto al momento dell'entrata in vigore della legge (prevista per il 1° luglio 2025). L'incaricato della protezione dei dati in carica al momento dell'entrata in vigore della legge eserciterà il proprio mandato sino all'entrata in vigore della legge e potrà poi essere riconfermato per il mandato successivo.

IV. Modifiche di altri atti normativi

La revisione totale apportata alla legge allo scopo di uniformarsi al diritto internazionale ha determinato la modifica o lo stralcio completo delle definizioni di alcuni termini (cfr. sopra art. 3 LCPD). Alcuni di questi adeguamenti terminologici non comportano modifiche materiali della situazione giuridica, in particolare lo stralcio ovvero la sostituzione del termine «collezione di dati». Pertanto, nei pochi punti del diritto grigionese in cui questi termini compaiono essi vengono adeguati nel quadro della revisione totale. Le altre modifiche apportate alla definizione dei termini possono determinare modifiche materiali della situazione giuridica. Ciò riguarda soprattutto le nuove categorie di dati personali degni di particolare protezione e la norma sulla profilazione. In questi casi occorre verificare nelle leggi settoriali che costituiscono il diritto materiale in materia di protezione dei dati se le basi legali vigenti sono sufficienti per trattamenti esistenti che interessano le corrispondenti categorie di dati. Tale verifica non sarà effettuata nel quadro del presente progetto legislativo (cfr. sopra art. 41). In relazione all'attuazione della direttiva 2016/680 nel diritto cantonale, sarà però imperativamente necessario procedere ad adeguamenti di leggi esistenti. Questa direttiva si applica alle autorità preposte al perseguimento di reati e all'esecuzione di sanzioni penali (cfr. art. 3 n. 7 direttiva 2016/680). Di regola i rispettivi adeguamenti possono essere apportati a livello di ordinanza (cfr. sopra art. 22 e 23). Data la prossimità tematica, il progetto di legge prevede inoltre l'adeguamento delle norme vigenti in materia di consultazione degli atti di procedimenti conclusi.

1. Legge sulla cittadinanza del Cantone dei Grigioni (LCCit; CSC 130.100)

Nell'art. 24 cpv. 1 LCCit si parla di «besonders geschützten Personendaten». Questo termine non compare in questa formulazione nel diritto in materia di protezione dei dati, né secondo la situazione giuridica previgente né secondo quella attuale. Nella versione tedesca esso deve essere perciò adeguato alla terminologia della LCPD e sostituito con «besonders schützenswerte Personendaten». In italiano si è proceduto a due piccoli adeguamenti linguistici.

2. Legge d'applicazione del Codice di diritto processuale civile svizzero (LACPC; CSC 350.100)

Art. 14 cpv. 4 Conservazione e consultazione degli atti

La LACPC disciplina la consultazione di atti di procedure civili concluse. La rispettiva norma prevale sulla LCPD in quanto diritto settoriale in materia di protezione dei dati (cfr. art. 3 cpv. 3). Attualmente la norma prevede l'impugnazione delle relative decisioni dinanzi all'autorità di

vigilanza della rispettiva autorità. In base a questa norma, le decisioni del Tribunale d'appello in materia di diritto di consultazione degli atti di procedure concluse dovrebbero essere impugnate dinanzi al Gran Consiglio. Tale norma risulta problematica in vista di una possibile impugnazione della rispettiva decisione dinanzi al Tribunale federale. Quali atti dell'amministrazione della giustizia, le decisioni concernenti il diritto di consultazione degli atti di procedure concluse devono essere impugnate con ricorso in materia di diritto pubblico dinanzi al Tribunale federale. Il ricorso in materia di diritto pubblico è ammesso contro decisioni delle autorità cantonali di ultima istanza; i Cantoni sono tenuti a istituire tribunali superiori quali autorità di grado immediatamente inferiore al Tribunale federale (art. 86 cpv. 2 LTF). A questo principio si può derogare soltanto nel caso in cui le decisioni abbiano carattere prevalentemente politico, cosa che non si può affermare per le fattispecie in oggetto. Per consentire l'impugnazione dinanzi al Tribunale federale, in virtù dell'art. 49 cpv. 1 lett. g LGA casi di questo tipo dovrebbero eventualmente essere giudicati di nuovo dal Tribunale d'appello dopo il passaggio in Gran Consiglio. Per evitare periodi di inattività formalistici, sarebbe più opportuno designare come definitive le decisioni del Tribunale d'appello, con possibilità di verifica comunque consentita esclusivamente al Tribunale federale. In misura minore, la stessa problematica si riscontra anche per il Tribunale di giustizia istituito con la riforma della giustizia 3. Anche le sue decisioni dovrebbero pertanto essere considerate definitive.

3. Legge d'applicazione del Codice di diritto processuale penale svizzero (LACPP; CSC 350.100)

Art. 36 cpv. 4 Conservazione e consultazione degli atti

L'art. 36 cpv. 4 LACPP prevede, analogamente all'art. 14 cpv. 4 LACPC, una disposizione concernente l'iter legale relativo alle decisioni in merito al diritto di consultazione degli atti in procedimenti conclusi. Questa disposizione deve essere modificata in maniera analoga per i motivi sopra esposti (cfr. osservazioni relative all'art. 14 LACPC).

4. Legge sulla vigilanza finanziaria (LVF; CSC 710.300)

Il termine «collezione di dati» non compare più nel nuovo diritto e deve pertanto essere sostituito dal termine «banca dati» anche in questa legge speciale. Ciò non determina modifiche materiali.

V. Conseguenze a livello finanziario e di personale

1. Per il Cantone

Le novità nel diritto sulla protezione dei dati necessarie a seguito dell'adeguamento al diritto internazionale comportano un certo onere supplementare. Nell'approccio attuativo si è cercato di sfruttare appieno i margini di manovra accordati dalla legislazione di rango superiore e di incorporare soltanto le direttive cogenti. Ad esempio, gli strumenti previsti dalla direttiva 2016/680 (registro delle attività di trattamento, consulente per la protezione dei dati) sono di applicazione esclusivamente per gli organi pubblici soggetti a questa direttiva. Altri obblighi, come l'obbligo di notificare le violazioni della sicurezza dei dati o di effettuare una valutazione d'impatto sulla protezione dei dati, devono però essere attuati da tutti gli organi soggetti alla legge. Si presume che questi strumenti e questi obblighi possano essere introdotti nell'Amministrazione cantonale impiegando le risorse esistenti. La funzione del consulente

per la protezione dei dati, prevista obbligatoriamente per determinate autorità, non comporta la creazione di nuovi posti di lavoro bensì maggiori compiti per i collaboratori esistenti. A questi ultimi viene richiesto di acquisire una certa competenza nell'ambito della protezione dei dati e di fungere da interlocutori nella comunicazione con l'organo di vigilanza.

L'organo di vigilanza a sua volta è in grado di adempiere i propri compiti in modo indipendente soltanto se gli sono assegnate le risorse necessarie per il loro espletamento. L'incaricato cantonale della protezione dei dati lavora attualmente con un grado di occupazione del 50% e riceve un compenso forfettario fisso con il quale devono essere coperte anche tutte le altre spese (ad es. di segreteria e per i locali). La revisione assegna all'organo di vigilanza nuovi compiti e nuove competenze. I fondi precedentemente stanziati difficilmente saranno sufficienti a coprire le spese necessarie in futuro per l'adempimento efficace delle mansioni tuttora esistenti, ma soprattutto dei nuovi compiti. La CdC raccomanda già ai piccoli Cantoni di prevedere una percentuale di impiego compresa tra il 50 e il 100 per cento (guida CdC, pag. 27). I Cantoni di dimensioni paragonabili ai Grigioni sono dotati di organi di vigilanza con percentuali di impiego comprese tra il 160 e il 590 per cento.[4] Sebbene queste autorità svolgano, in alcuni casi, anche altri compiti (ad es. in qualità di incaricati della trasparenza) e sebbene questi Cantoni abbiano requisiti diversi, è comunque chiaro che l'attuale organo di vigilanza è dotato di una percentuale d'impiego troppo bassa. Ciò risulta ancora più evidente se si considera che (a differenza di quanto avviene in alcuni Cantoni) l'organo di vigilanza si occupa anche della vigilanza sugli attuali 101 comuni. Per questo motivo, nel quadro della revisione della legge sulla protezione dei dati deve essere aumentata anche la percentuale d'impiego dell'incaricato della protezione dei dati. A seguito dei nuovi compiti, la funzione dell'incaricato della protezione dei dati deve corrispondere a un impiego all'80 – 100 per cento. In aggiunta dovrà essere assunto in funzione di supplente anche un nuovo collaboratore (50 – 70 %). Inoltre potrebbe essere necessario assumere una persona che svolgerà compiti amministrativi (20 – 50%). Finora le spese derivanti dai lavori di segreteria erano retribuite con un compenso forfettario. In sintesi, con l'entrata in vigore della legge e la contestuale introduzione di nuovi compiti a carico dell'organo di vigilanza si ipotizza un aumento del fabbisogno di impiego pari al 100 – 170 per cento.

Al momento non è ancora possibile quantificare esattamente gli oneri supplementari derivanti dalla nuova legislazione, non essendo ad esempio ancora note le descrizioni concrete degli impieghi e dunque la classificazione delle potenziali persone da assumere. Sinora all'incaricato della protezione dei dati era stato riconosciuto nel conto annuale un importo forfettario annuo di circa 160'000 franchi, comprendente, oltre al compenso per il titolare della carica, anche tutti gli altri costi associati alle sue attività (amministrazione, consultazione di esperti esterni, spese materiali). In futuro per la retribuzione dell'incaricato della protezione dei dati e dei suoi collaboratori è previsto che si prenda come riferimento il diritto cantonale del personale (cfr. anche art. 34). Stando ai gradi di occupazione proposti, i costi salariali dovrebbero ammontare presumibilmente a circa 350'000 franchi (compresi i contributi alla Cassa pensioni e alle assicurazioni sociali) per finanziare, nel complesso, l'incremento delle

[4] BL: 530 per cento di impiego; BS: 590 per cento di impiego, SO: 360 per cento di impiego, SZ/OW/NW: 180 per cento di impiego, ZG: 260 per cento di impiego (le cifre sono riprese dai rapporti annuali delle rispettive autorità per l'anno 2022).

percentuali di impiego dell'incaricato, l'assunzione di uno specialista in ambito giuridico o informatico in veste di supplente ed eventualmente l'assunzione di un collaboratore di segreteria. A queste spese si aggiungono i costi per gli uffici, i materiali, ecc., sinora sempre ricompresi nell'importo forfettario riconosciuto all'incaricato. Gli oneri supplementari dovrebbero dunque raggiungere la cifra di 300'000 franchi all'anno.[5]

2. Per i comuni e le regioni

Gli organi e gli uffici pubblici di regioni e comuni sono soggetti alla LCPD. In virtù dei nuovi obblighi istituiti (obbligo di notifica in caso di violazioni della sicurezza dei dati, valutazioni d'impatto sulla protezione dei dati), anche loro dovranno attendersi un certo onere supplementare. Se sarà possibile rispondervi con le risorse esistenti dipende dalle dimensioni dell'amministrazione comunale.

VI. Buona legislazione

Il progetto rispetta i principi della "buona legislazione" conformemente alle direttive del Governo (cfr. decreto governativo del 16 novembre 2010, prot. n. 1070/2010).

[5] Stando ai rispettivi rapporti annuali o rapporti di attività, gli organi di vigilanza dei Cantoni summenzionati operano con un budget compreso tra 500'000 e 1,3 milioni di franchi.