CONSIGLIO REGIONALE DEL PIEMONTE - Deliberazione dell'Ufficio di Presidenza

Deliberazione 18 dicembre 2025, n. 319

APPROVAZIONE DEL PIANO DI GESTIONE DEGLI INCIDENTI DI CYBERSICUREZZA (ARTICOLO 25 D.LGS. 138/2024) E DELLE ISTRUZIONI OPERATIVE E PROCEDURALI IN MATERIA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH - ARTICOLI 32, 33 E 34 REG. (UE) 2016/679). (CG/FDA)

Documento allegato

CONSIGLIO REGIONALE DEL PIEMONTE

Ufficio di Presidenza

Delibera n. 319/2025 - Cl. 6.6.4 - 6.4.2

Oggetto APPROVAZIONE DEL PIANO DI GESTIONE DEGLI INCIDENTI DI CYBERSICUREZZA (ARTICOLO 25 D.LGS. 138/2024) E DELLE ISTRUZIONI OPERATIVE E PROCEDURALI IN MATERIA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH - ARTICOLI 32, 33 E 34 REG. (UE) 2016/679). (CG/FDA)

Seduta n. 50

L'anno 2025, il giorno 18 dicembre alle ore 13.53 - presso la sede di Palazzo Lascaris, via Alfieri n. 15, Torino - si è riunito l'Ufficio di Presidenza del Consiglio Regionale.

Sono presenti: il Presidente NICCO, il Vice Presidente GRAGLIA, i Consiglieri Segretari CAROSSO, CERA.

Non sono presenti: il Vice Presidente RAVETTI, il Consigliere Segretario CASTELLO.

A relazione del Presidente NICCO

APPROVAZIONE DEL PIANO DI GESTIONE DEGLI INCIDENTI DI CYBERSICUREZZA (ARTICOLO 25 D.LGS. 138/2024) E DELLE ISTRUZIONI OPERATIVE E PROCEDURALI IN MATERIA DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH - ARTICOLI 32, 33 E 34 REG. (UE) 2016/679). (CG/FDA)

Premesso che:

- il Parlamento europeo e il Consiglio, in data 14 dicembre 2022, hanno approvato la Direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148, di seguito direttiva NIS 2;
- tutti gli Stati membri erano tenuti a recepire la direttiva NIS 2, entrata in vigore in data 17 gennaio 2023, entro il 17 ottobre 2024;
- con decreto legislativo 4 settembre 2024, n. 138 “Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 delle violazioni dei dati personali”, di seguito decreto NIS 2, è stata recepita la direttiva;
- la direttiva NIS 2 introduce misure volte a garantire un elevato livello generale di cybersicurezza nell’Unione, in modo da migliorare il funzionamento del mercato interno, e definisce una serie di obblighi e misure da adottare da parte degli Stati membri;
- l’Agenzia per la Cybersicurezza Nazionale il 12 aprile 2025 ha individuato il Consiglio regionale del Piemonte quale “soggetto importante”, come definito dall’art. 6 del “decreto NIS 2";
- in data 30 luglio 2025, l’Ufficio di Presidenza, con la deliberazione n. 198, ha dato una prima attuazione a quanto stabilito dagli articoli 7 e 23 del d.lgs. n. 138 del 2024;
- il Parlamento europeo e il Consiglio europeo, in data 27 aprile 2016, hanno approvato il Regolamento (UE) 2016/679 (GDPR-General Data Protection Regulation), di seguito GDPR, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi;
- il GDPR, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, dopo un periodo di transizione di due anni, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;
- con decreto legislativo 10 agosto 2018, n. 101 “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016”, il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) è stato adeguato alle disposizioni del GDPR;
- in data 23 luglio 2025, l’Ufficio di Presidenza, con la deliberazione n. 189, ha approvato la nuova versione del registro delle attività di trattamento del titolare ed ha aggiornato il sistema di gestione della funzione inerente alla protezione dei dati personali, integrando e modificando quanto previsto originariamente dalla deliberazione n. 113 del 2018;
- la deliberazione n. 189/2025 ha altresì disposto, al fine di garantire la corretta osservanza degli obblighi discendenti dal GDPR e dalla normativa nazionale, la costituzione di un organismo tecnico stabile, denominato “Gruppo dei referenti privacy”, preposto allo svolgimento di compiti operativi;

Considerato che:

- il d.lgs. n. 138 del 2024 impone ai soggetti qualificati come “soggetti importanti” l’adozione di misure minime di sicurezza, organizzative e tecniche, tra cui vi sono quelle inerenti alla procedura per la gestione degli incidenti e la notifica degli incidenti significativi, come previsto dall’articolo 25;
- l'articolo 32 del GDPR stabilisce che il titolare e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;
- lo stesso articolo 32 prevede altresì che, nel valutare l'adeguato livello di sicurezza, si debba tenere conto, in special modo, dei rischi presentati dal trattamento che derivano anche dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- l’articolo 33 del GDPR prevede l'obbligo di notifica all'autorità di controllo in caso di violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche e l'articolo 34 stabilisce che il titolare del trattamento è tenuto a comunicare all'interessato la violazione senza ingiustificato ritardo, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- con la deliberazione n. 273 del 28 dicembre 2018, l’Ufficio di Presidenza ha dato attuazione a quanto previsto dagli articoli 32, 33 e 34 del GDPR, ed ha approvato sia le istruzioni operative per l’utilizzo dei dispositivi informatici, dei servizi digitali e della gestione documentale nell’attività lavorativa - aggiornate e sostituite con le deliberazioni n. 101 del 17 giugno 2021 e n. 108 del 23 maggio 2024 - sia la procedura di gestione del Data Breach del Consiglio regionale del Piemonte, nonché le Misure di sicurezza implementate per garantire la sicurezza dei dati personali;

Ritenuto necessario adottare con un unico documento (**Allegato A**), facente parte integrante e sostanziale della presente deliberazione, il piano di gestione degli incidenti di cybersicurezza previsto dall’articolo 25 del d.lgs. n. 138 del 2024 e quello inerente alla gestione della violazione dei dati personali (Data Breach), di cui agli articoli 33 e 34 del GDPR, dato che risultano tra loro strettamente correlati e denotano una sostanziale complementarietà;

Dato atto nondimeno delle competenze dei soggetti individuati “organi amministrativi e direttivi” dalla deliberazione dell’Ufficio di Presidenza 30 luglio 2025, n. 198, relative all’approvazione

delle modalità di implementazione delle misure nell'ambito del perimetro NIS 2, prima tra tutte la gestione degli incidenti di cybersicurezza;

Valutato quindi di approvare l'**Allegato A** per le parti inerenti alla violazione di dati personali (Data Breach-Articoli 33 e 34 del GDPR), subordinando l'efficacia delle parti relative alla gestione degli incidenti di cybersicurezza all'adozione, da parte dei soggetti individuati "organi amministrativi e direttivi" dalla deliberazione dell'Ufficio di Presidenza 30 luglio 2025, n. 198 degli atti di rispettiva competenza;

Ritenuto altresì di ricomprendere nella presente deliberazione, al fine di garantire la massima organicità e chiarezza sistematica, anche le istruzioni operative ai sensi dell'articolo 32 del GDPR per l'utilizzo dei dispositivi informatici, dei servizi digitali e della gestione documentale nell'attività lavorativa (**Allegato B**), facente parte integrante e sostanziale della presente deliberazione;

Valutato che le misure di sicurezza adottate con la citata deliberazione n. 273 del 2018 sono ora contenute nella nuova versione del registro delle attività di trattamento del titolare, approvato con la deliberazione n. 189 del 2025, e che quindi i contenuti e gli allegati della deliberazione n. 273 del 2018 e delle deliberazioni di modifica n. 101 del 2021 e n. 108 del 2024 sono integralmente trasfusi nel presente provvedimento, che ne costituisce disciplina aggiornata e sostitutiva;

Considerato opportuno, per quanto sopra esposto, disporre la cessazione degli effetti delle citate deliberazioni a decorrere dalla data di approvazione del presente atto;

Ritenuto altresì di demandare ad atti dirigenziali successivi l' adozione degli adempimenti necessari e conseguenti;

Vista la deliberazione dell'Ufficio di Presidenza n. 318 del 18/12/2025 "Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del d.lgs. 138/2024 in Consiglio regionale del Piemonte. Approvazione";

L'Ufficio di Presidenza, all'***unanimità dei presenti***,

D E L I B E R A

1. di dare atto che le premesse costituiscono parte integrante e sostanziale della presente deliberazione;

2. di approvare, allegandolo a questa deliberazione per farne parte integrante e sostanziale (**Allegato A**), il "Piano di gestione degli incidenti di cybersicurezza (art. 25 d.lgs. 138/2024) e delle violazioni di dati personali" (data breach - artt. 33 e 34 Reg. (UE) 2016/679) per le parti inerenti alla violazione di dati personali (data breach - articoli 33 e 34 del GDPR), subordinando l'efficacia delle parti relative alla gestione degli incidenti di cybersicurezza all'adozione, da parte dei soggetti individuati "organi amministrativi e direttivi" dalla deliberazione dell'Ufficio di Presidenza 30 luglio 2025, n. 198, degli atti di rispettiva competenza;

3. di approvare le istruzioni operative e procedurali, ai sensi dell' articolo 32 del GDPR, allegate a questa deliberazione per farne parte integrante e sostanziale (**Allegato B**);

4. di dare mandato agli uffici di pubblicare gli **Allegati A** e **B** nella Intranet del sito istituzionale del Consiglio regionale nonché di predisporre e notificare apposito ordine di servizio;

5. di demandare ad atti dirigenziali successivi l'adozione degli adempimenti necessari e conseguenti;

6. di disporre la cessazione degli effetti delle deliberazioni dell' Ufficio di Presidenza n. 273 del 2018, n. 101 del 2021 e n. 108 del 2024.

Piano di gestione degli incidenti di cybersicurezza (art. 25 D.lgs. 138/2024) e delle violazioni di dati personali (data breach - artt. 33 e 34 Reg. (UE) 2016/679)

1 Sommario

2 Scopo del documento

Il presente documento contiene le disposizioni procedurali del Consiglio regionale del Piemonte riguardo alla gestione degli incidenti in materia di cybersicurezza, ai sensi della Direttiva (UE) 2022/2555 (Network and Information Security - NIS 2) e del Decreto legislativo 4 settembre 2024, n. 138, nonché delle violazioni dei dati personali.

Le violazioni di dati personali o data breach, ai sensi del Regolamento (UE) 2016/679 (GDPR), costituiscono una specifica tipologia di incidente di sicurezza informatica ma possono verificarsi anche in forma cartacea qualora la violazione riguardi documenti cartacei contenenti dati personali.

In precedenza, le disposizioni procedurali del Consiglio regionale del Piemonte in materia di gestione degli incidenti di sicurezza e delle violazioni dei dati personali erano contenute negli allegati della deliberazione dell'Ufficio di Presidenza n. 273 del 2018. I contenuti e gli allegati di tale deliberazione sono integralmente trasfusi nel provvedimento di approvazione di questo documento, poiché si è ritenuto opportuno, al fine di garantire la massima organicità e chiarezza sistematica, di adottare un unico piano di gestione degli incidenti di cybersicurezza, previsto dall'art. 25 del D.lgs. 138 del 2024, e delle violazioni dei dati personali (data breach), di cui agli articoli 33 e 34 del GDPR.

Ai fini del presente documento, le espressioni sicurezza informatica e cybersicurezza sono utilizzate in modo coordinato: con sicurezza informatica si fa riferimento all'organizzazione interna e ai presìdi operativi dell'Ente, mentre con cybersicurezza si richiama in particolare il quadro normativo europeo e nazionale (Direttiva NIS 2 e relativa disciplina di attuazione). Nei passaggi in cui non vi siano possibili ambiguità, i due termini possono essere considerati equivalenti.

3 Riferimenti normativi

Nella redazione del presente documento, oltre che dalla lettura della Direttiva (UE) 2022/2555 (NIS 2) e del Decreto legislativo 4 settembre 2024, n. 138, nonché per le violazioni dei dati personali del Regolamento (UE) 2016/679 e del D.Lgs. 30 giugno 2003 n. 196, come modificato ed integrato dal D.Lgs. 10 agosto 2018 n.101, sono state tratte notizie e/o incorporati documenti redatti da:

- Linee guida del gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata);
- Good Practice Guide for Incident Management, Agenzia dell'Unione europea per la cibersicurezza (ENISA) 2010;
- Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali adottate dall'Autorità Garante per la protezione dei dati personali con provvedimento n. 221 del 26/07/2012 (G.U. n. 183 del 07/08/2012 – doc. web n. 1915485);
- Raccomandazioni per una metodologia di valutazione della gravità delle violazioni dei dati personali, Agenzia dell'Unione europea per la cibersicurezza (ENISA) 2013;
- Guida all'applicazione del GDPR resa disponibile dall'autorità nazionale Garante per la protezione dei dati personali;
- Provvedimento del Garante nazionale per la protezione dei dati personali in materia della disciplina sulla comunicazione dei dati personali (c.d. "data breach") del 04/04/2013 (G.U. n. 97 del 26/04/2013 – doc. web 2388260);
- Provvedimento del Garante sulla notifica delle violazioni dei dati personali (data breach) - 30 luglio 2019- doc. web n.9126951;
- Linee guida EDPB 01/2021 sugli esempi riguardanti la notifica di violazione dei dati;
- Linee guida 9/2022 EDPB in materia di notifica delle violazioni di dati personali (data breach), adottate il 28-03-2023;
- Determinazione ACN 164179 del 14 aprile 2025 – Specifiche di base per l'adempimento agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS;

- Linee Guida NIS dell'ACN "Specifiche di base-Guida alla lettura";
- Guida dell'ACN alla notifica degli incidenti al CSIRT Italia;
- Interventi e materiale resi disponibili dalla Regione Piemonte in collaborazione con il CSI Piemonte, l'ANCI, l'UNCEM ed alcuni Enti Piemontesi.

4 Glossario

- **NIS 2: Direttiva (UE) 2022/2555** del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa alle misure per un livello elevato comune di sicurezza delle reti e dei sistemi informativi nell'Unione europea. Ai fini del presente documento, per semplicità espositiva, il termine "NIS" è utilizzato in forma abbreviata per riferirsi alla Direttiva (UE) 2022/2555 (*NIS 2*) e alla relativa disciplina nazionale di attuazione.
- **Decreto legislativo NIS**: è il Decreto legislativo n. 138 del 2024 di recepimento della Direttiva (UE) 2022/2555 (NIS 2) e disciplina nazionale per la gestione della sicurezza delle reti e dei sistemi informativi.
- **Soggetto essenziale**: quello che svolge servizi essenziali per la società e l'economia e che, in caso di interruzione, potrebbe causare gravi disagi.
- **Soggetto importante**: ente privato o pubblico per il quale la conformità alla NIS è fondamentale per garantire la sicurezza dei dati e la continuità dei servizi.
- **Punto di contatto**: è la figura istituzionale che l'organizzazione designa verso l'ACN. E' il soggetto che sovrintende l'attuazione del decreto NIS, effettua la registrazione ed inserisce le informazioni nel portale ACN dedicato allo scambio di informazioni relative al "Decreto NIS", cura i rapporti con l'Agenzia per la Cybersicurezza Nazionale (ACN) per conto del soggetto NIS;
- **Sostituto del punto di contatto**: soggetto individuato ai sensi dell'articolo 7, comma 1, lettera c) del Decreto NIS, che svolge gli adempimenti necessari in caso di assenza o impedimento del Punto di contatto.
- **Referente CSIRT**: è la figura operativa, che cura i rapporti quotidiani con lo CSIRT Italia. Gestisce notifiche di incidenti, monitoraggio e comunicazioni tecniche. È una sorta di "ponte tecnico" tra l'organizzazione e il sistema nazionale di cybersicurezza.
- **CISO-Chief Information Security Officer**: il Responsabile della sicurezza informatica all'interno dell'organizzazione.
- **Organi amministrativi e direttivi**: sono gli organi aziendali o istituzionali che esercitano le funzioni decisionali e di direzione dell'ente (es. consiglio di amministrazione, amministratore unico, organo di vertice). Ai sensi dell'art. 23 del decreto NIS essi sono destinatari di obblighi di governance specifici in materia di sicurezza delle reti e dei sistemi informativi. Devono assicurare responsabilità e presidio della cibersicurezza a livello più alto dell'organizzazione; sovrintendere all'adempimento degli obblighi previsti, esercitando controllo e verifica sull'implementazione operativa delle misure richieste. Sono soggetti responsabili per le violazioni del decreto.
- **Asset**: risorsa informatica (hardware, software, dati, servizio) rilevante per la fornitura di un servizio essenziale o importante.
- **API** (Application Programming Interface): sono interfacce software che definiscono regole e protocolli per lo scambio di dati e comandi tra applicazioni, servizi e componenti; in ambito di cybersicurezza sono punti di ingresso e vettori di rischio perché mediano accesso a dati e funzionalità "nascoste" delle applicazioni o di un sito web
- **ACN: Agenzia per la Cybersicurezza Nazionale**. È l'autorità nazionale italiana istituita per tutelare gli interessi dello Stato nel cyberspazio e coordinare la protezione delle reti, dei sistemi informativi e dei servizi critici.
- **CSIRT Italia**: il gruppo nazionale di risposta agli incidenti cui le notifiche devono essere indirizzate secondo il D.Lgs. 138/2024
- **Contenimento**: misure temporanee adottate per limitare la diffusione o l'aggravamento dell'incidente.
- **DPO (Data Protection Officer)**: il responsabile della protezione dei dati personali, coinvolto quando l'incidente comporta trattamenti di dati personali.

- **GDPR o RGPD - Regolamento Europeo in materia di protezione dei dati personali** nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 e applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018. L'acronimo GDPR si riferisce al termine anglosassone "General Data Protection Regulation" mentre l'acronimo RGPD si riferisce alla definizione nazionale "Regolamento Generale sulla Protezione dei Dati".
- **Codice** - Codice nazionale in materia di protezione dei dati personali (D.Lgs 30 giugno 2003, n. 196)
- **Garante** - Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente, il GDPR identifica questa figura denominandola "Autorità di controllo" (vedasi artt. 51 ss del GDPR).
- **Titolare** – Titolare del trattamento - l'autorità che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.
- **Responsabile** – Responsabile del trattamento - soggetto pubblico o privato, che tratta dati personali per conto del Titolare del trattamento.
- **Data Breach** – evento in conseguenza del quale si verifica una "violazione dei dati personali". Con il termine "data breach" si intende un incidente di sicurezza in cui dati personali, sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. La casistica è molto estesa, un "data breach" si può anche verificare a seguito di un problema hardware o software o con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza (ad esempio, sul web) in maniera involontaria o volontaria, con il furto di dati, ecc..
- **Accountability** - principio per cui il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al GDPR.
- **Privacy by design** – principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione sia dell'esecuzione del trattamento.
- **Privacy by default** – principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative volte a tutelare la vita privata per "impostazione predefinita".
- **RACI** – standard di matrice per la definizione di ruoli e responsabilità per l'esecuzione di una determinata attività dove vengono poste in relazione le risorse con le attività che esse devono svolgere.
- **RTD** – Responsabile della transizione al digitale ai sensi dell'art. 17 CAD.
- **WP29** – gruppo di lavoro istituito in virtù dell'art. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata).
- **D-SOC** - Security operation center distribuito, unità organizzativa di CSI Piemonte dedicata alla sicurezza informatica

5 Principi di gestione e politiche

Il Consiglio regionale del Piemonte adotta un modello unificato di gestione degli incidenti di sicurezza informatici e dei data breach basato su principi di tempestività, trasparenza, responsabilità e miglioramento continuo.

Il modello si fonda sui seguenti principi di governance:

Centralità della gestione coordinata. Tutti gli incidenti di sicurezza informatica sono gestiti attraverso un processo integrato che coinvolge le funzioni tecniche, organizzative e direzionali sotto la supervisione del Chief Information Security Officer (CISO).

Accountability e responsabilità condivisa. Ogni funzione organizzativa è tenuta a cooperare con il CISO e con il Presidio per la cybersicurezza, segnalando tempestivamente ogni evento potenzialmente riconducibile a un incidente di sicurezza.

Tempestività e obblighi di notifica. In caso di incidenti significativi, l'Entel'Ente è tenuto alla notifica verso lo CSIRT Italia (ACN) secondo procedure e tempistiche prestabilite. La gestione degli incidenti deve prevedere, secondo la normativa vigente, una prima comunicazione, volta a fornire un avviso tempestivo e, se possibile, indicazioni preliminari sull'eventuale natura malevola dell'incidente o sul suo possibile impatto transfrontaliero. Successivamente deve essere inviata una notifica completa, aggiornata e contenente una valutazione iniziale della gravità e dell'impatto, nonché eventuali indicatori di compromissione. Durante tutto il ciclo di gestione dell'incidente possono essere predisposte relazioni intermedie su richiesta del CSIRT Italia, mentre deve essere predisposta una relazione finale, trasmessa entro i termini stabiliti, che descrive in dettaglio l'incidente, le cause o le minacce all'origine, le misure di contenimento adottate e l'evoluzione della situazione fino alla sua conclusione. Tutte le comunicazioni devono essere effettuate tempestivamente e secondo quanto previsto dalla normativa vigente, garantendo al CSIRT Italia una completa e corretta informazione.

Principio del "need-to-know" e riservatezza delle informazioni. Le informazioni relative agli incidenti sono condivise esclusivamente con i soggetti autorizzati e nel rispetto dei vincoli di riservatezza, integrità e protezione dei dati personali.

Integrazione con la continuità operativa e la gestione del rischio.

Analisi e miglioramento continuo. Ogni incidente significativo è oggetto di una revisione post-evento ("lessons learned") finalizzata a individuare azioni preventive, aggiornare le procedure e migliorare le misure tecniche e organizzative.

Cultura della sicurezza e formazione. Il Consiglio regionale promuove la consapevolezza e la formazione continua del personale e dei fornitori, affinché ogni soggetto sia in grado di riconoscere, segnalare e gestire correttamente un potenziale incidente.

Corresponsabilità organizzativa. La gestione degli incidenti di sicurezza informatica è una responsabilità estesa a tutte le funzioni dell'Ente. Ogni funzione del Consiglio regionale, indipendentemente dal proprio ruolo tecnico, amministrativo o gestionale, contribuisce attivamente alla prevenzione, alla segnalazione e alla corretta comunicazione degli incidenti.

6 Ruoli e responsabilità: il Presidio per la cybersicurezza e la protezione dei dati del Consiglio regionale

Il modello di governance degli incidenti di sicurezza del Consiglio regionale del Piemonte si basa su una struttura multilivello, che assicura la responsabilità diretta degli organi di vertice e una chiara distinzione tra ruoli decisionali, di coordinamento e operativi. La gestione degli incidenti informatici e delle violazioni dei dati personali (data breach) era già presente nell'Ente ed è stata, da ultimo, regolamentata dalla deliberazione n. 273 del 2018, già richiamata in apertura del presente documento.

Il gruppo di persone cui è affidato il governo del processo di gestione degli incidenti significativi di cybersicurezza è denominato '**Presidio per la cybersicurezza e la protezione dei dati'** ed è composto dalla Segretaria Generale, dal Direttore Responsabile della transizione digitale (RTD), dal Dirigente responsabile della struttura organizzativa nella quale si verifica l'incidente, dal CISO, ovvero il Responsabile della sicurezza informatica, coincidente nel caso del Consiglio regionale con il Responsabile dei sistemi informativi, il Punto di Contatto del Consiglio regionale, dal Sostituto del Punto di contatto, dal Referente CSIRT e dal DPO.

Nel caso in cui l'incidente sia qualificabile come Data Breach, oltre al Presidio sopra illustrato, sono coinvolte anche le figure del Responsabile della gestione documentale, la Coordinatrice, la Segretaria e i componenti del Gruppo dei referenti privacy di settore.

Si precisa inoltre che il Consiglio regionale del Piemonte si avvale del CSI Piemonte per la gestione tecnica della sicurezza informatica dei sistemi informativi e di rete inclusi nel perimetro dell'affidamento in house.

I ruoli coinvolti sono definiti nel documento "Organizzazione per la sicurezza informatica"; qui di seguito si riprende l'elenco riepilogativo e lo si integra con i ruoli rientranti nella gestione della protezione dei dati personali:

- Titolare (Ufficio di Presidenza);
- Contitolare (Gruppi consiliari e Corecom);
- Garanti e Difensore Civico;
- Direttori/Segretaria Generale delegati all'attuazione del trattamento dati sul quale avviene la segnalazione di incidente di sicurezza;
- Dirigente delegato all'attuazione del trattamento dati sul quale avviene la segnalazione di incidente di sicurezza;
- Responsabile Transizione al Digitale;
- Responsabile Sistemi informativi;
- Responsabile Sicurezza informatica (CISO);
- Funzionari del settore Sistemi informativi;
- Punto di contatto NIS;
- Sostituto punto di contatto NIS;
- Referente CSIRT;
- Responsabile protezione dati (DPO);
- Referenti privacy di settore;
- Coordinatrice dei referenti privacy;
- Segretaria tavolo referenti privacy;
- Responsabile trattamento esterno;
- Fornitore;
- Responsabile Sicurezza informatica (CISO) di CSI Piemonte;
- D-SOC (Security operation center distribuito) di CSI Piemonte;
- Presidi tecnici di CSI Piemonte;
- Responsabile archivio / gestione documentale;
- Soggetto interessato dalla violazione;
- Forze dell'ordine;
- ACN;
- CSIRT;
- Garante Privacy.

7 Procedura di gestione degli incidenti significativi in materia di cybersicurezza e dei data breach

Nei paragrafi seguenti vengono dettagliate le attività eseguite in ciascuno dei passi del processo di gestione, prima, degli incidenti di cybersicurezza, e poi dei data breach.

Gli elementi del processo di gestione riconducibili a fattispecie comuni sono descritti congiuntamente.

Un incidente è **significativo** in ambito NIS, dunque soggetto all'obbligo di notifica, quando ha causato o è in grado di causare un impatto significativo sulla continuità, sulla disponibilità, sull'integrità o sulla riservatezza dei servizi essenziali o dei sistemi informativi; la soglia di rilevanza si valuta in base a parametri tecnici, operativi e impatti su utenti, terzi o infrastrutture critiche.

Il **data breach** invece è un particolare incidente di sicurezza che comporta "accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4 par. 12 GDPR).

Gli eventi che possono comportare un incidente di sicurezza e/o un data breach possono essere, ad esempio:

- interruzione massiva del servizio;
- compromissione di supply chain / terze parti come, ad esempio, la violazione di un fornitore cloud, di un componente software o di servizi esterni che si propaga ai sistemi dell'ente e ne riduce affidabilità o sicurezza;
- compromissione di caselle di posta elettronica;
- attacchi mirati di phishing/social engineering con conseguente compromissione;
- incidenti fisici con ripercussione digitale,incendi, allagamenti;
- uso illecito di API o abuso di funzionalità esposte, sfruttamento
- Sfruttamento di API per estrarre dati in massa, alterare stati applicativi o sovraccaricare servizi;
- manipolazione dell'integrità dei dati come, ad esempio, l'alterazione fraudolenta di database;
- compromissione di infrastrutture di rete fondamentali (DNS, BGP), manipolazione rotte o altri eventi che interrompono accesso o reindirizzano traffico in modo dannoso;
- data Exfiltration (copia o trasferimento non autorizzati di dati);
- ransomware/malware;
- distruzione accidentale archivio digitale;
- smarrimento, furto di PC o server;
- smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.);
- smarrimento, furto o distruzione di un archivio cartaceo.

A fronte della segnalazione di un evento che può comportare un incidente di sicurezza e/o un data breach, viene attivata la presente procedura.

Gli eventi possono essere segnalati da soggetti interni o esterni, dalle forze dell'ordine o dal Garante stesso.

8 Fasi comuni della procedura

8.1 Fase 1 - Rilevazione della segnalazione e dell'evidenza di un incidente rilevante di cybersicurezza

Per evidenza si intende il momento in cui il soggetto dispone di elementi oggettivi dai quali si evince che si è verificato un incidente di sicurezza informatica.

L'acquisizione dell'evidenza definisce il momento dal quale decorre il termine per adempiere all'obbligo di notifica.

L'evidenza di un incidente viene generalmente acquisita tramite:

- analisi di segnalazioni fatte da attori esterni al soggetto, come ad esempio quelle effettuate dal CSIRT Italia;
- analisi di segnalazioni fatte da attori interni al soggetto, come ad esempio quelle di un utente che riporta un malfunzionamento al servizio di help desk;
- analisi degli eventi di sicurezza rilevati dai sistemi di monitoraggio.

La prima fase nella gestione del "data breach" è quella che porta a conoscenza della violazione o presunta violazione di sicurezza e della sua comunicazione al Titolare.

Le modalità con cui si viene a conoscenza del verificarsi di un incidente di sicurezza e/o di un "data breach" sono molteplici e non enumerabili in modo esaustivo; a puro titolo di esempio una segnalazione può pervenire:

- dagli addetti all'amministrazione dei sistemi informativi;
- da personale interno all'ente;
- da parte di organi pubblici (altri enti, Polizia, Carabinieri, Magistratura, ecc.);
- da parte dei soggetti esterni incaricati all'esecuzione di trattamenti (o parti di essi) per conto del Consiglio regionale;
- da parte di cittadini o comunque di soggetti privati esterni all'ente;
- fornitori.

È importante che la raccolta della segnalazione o l'esecuzione della segnalazione da parte degli uffici avvenga raccogliendo quante più informazioni possibile (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc.).

Nel caso in cui la segnalazione sia raccolta da persone fisiche è opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sul/i segnalatori (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica).

Anche le segnalazioni anonime e/o verbali devono essere raccolte ed inviate al titolare per consentire a quest'ultimo di accertare la reale sussistenza della violazione, disporre l'eventuale notifica o le comunicazioni ed assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

Non appena si viene a conoscenza di un incidente di sicurezza o di una violazione dei dati personali, al momento del verificarsi del fatto o della sua scoperta, il dipendente - o altro utente dei servizi informatici del Consiglio - che ha ricevuto la segnalazione oppure che è incorso direttamente nell'evento deve attenersi alla procedura di segnalazione approvata dal direttore competente in materia di sistemi informativi e transizione digitale, che disciplina le modalità e i destinatari delle comunicazioni, sia per gli incidenti relativi ai sistemi informatici sia per quelli che coinvolgono archivi cartacei.

Qualora la segnalazione pervenga da un responsabile esterno del trattamento, da un altro organismo pubblico o da un servizio interno, il personale del Consiglio è tenuto a gestirla secondo la medesima procedura, nel rispetto di quanto previsto dall'art. 33, paragrafo 2, del GDPR.

Tutte le segnalazioni di incidenti di sicurezza e/o di data breach di cui si viene a conoscenza sono inserite nell'apposito registro, secondo le modalità stabilite dalla procedura sopra citata.

8.2 Fase 2 - Analisi e gestione tecnica dell'incidente

In seguito, si passa al triage inziale e al contenimento temporaneo, cioè da un lato si identifica cosa è successo, quando, quali sistemi/servizi sembrano coinvolti, si raccolgono evidenze immediate si cerca di identificare la natura dell'incidente (malware, ransomware, data breach, disponibilità, integrità, riservatezza) e di applicare misure temporanee di contenimento per limitare l'aggravamento.

A fronte di una segnalazione viene eseguita un'attività di indagine ed investigazione per determinare se effettivamente c'è stata una violazione dei dati personali. Tale attività è condotta dal Presidio di sicurezza del Consiglio regionale e dove necessario dal responsabile esterno, la responsabilità è in capo ai delegati all'attuazione del trattamento.

9 Fasi della procedura di gestione incidenti di cybersicurezza

9.1 Fase 3 - Contenimento e Mitigazione

Prevede l'attivazione di misure tecniche e organizzative per limitare la propagazione dell'incidente e ridurre l'impatto. Le azioni possono includere, ad esempio, l'isolamento di sistemi compromessi, il blocco di account, l'applicazione di patch di sicurezza, la revoca di account o privilegi utente.

9.2 Fase 4 - Comunicazione e Notifica

Prevede la gestione delle comunicazioni interne ed esterne, inclusa la notifica obbligatoria allo CSIRT Italia entro le tempistiche di legge. In caso di data breach, si applicano anche le disposizioni del GDPR; si rimanda per i dettagli alla procedura di gestione dei data breach.

Si rimanda al par. *Gli incidenti significativi in materia di cybersicurezza e i data breach* per la descrizione dettagliata del processo di comunicazione.

9.3 Fase 5 - Risoluzione, Ripristino e Chiusura

Prevede il ripristino dei servizi e la normalizzazione degli ambienti impattati al fine di riprendere la normale operatività. Questa fase può includere attività di analisi forense digitale per individuare le cause e raccogliere

prove utili ai fini delle comunicazioni alle Autorità. Ripristinati i servizi viene gestita la comunicazione di chiusura dell'incidente verso tutti i soggetti coinvolti e/o impattati.

9.4 Fase 6 - Reporting e Miglioramento Continuo

Prevede la redazione della documentazione completa dell'incidente, l'analisi delle cause radice e la definizione di azioni correttive. Le lezioni apprese vengono integrate nel piano di sicurezza e nelle procedure operative, secondo il ciclo PDCA (Plan-Do-Check-Act).

10 Fasi della procedura di gestione dei data breach

10.1 Fase 3 – Valutazione del data breach

A fronte dell'accertamento di un data breach su dati di titolarità del Consiglio regionale, è necessario procedere alla valutazione dei rischi (o meglio del "livello di severità" dell'incidente) in considerazione degli effetti che la violazione di sicurezza può comportare sui diritti e le libertà delle persone.

Devono essere soppesate la "probabilità, focalizzata sul concreto rischio per la privacy, e la gravità degli effetti del rischio" come elemento decisivo nella scelta di notificare o meno. Occorre dunque svolgere una valutazione concreta e documentata della probabilità e della gravità del rischio per i diritti e le libertà delle persone interessate, prendendo in considerazione sia la gravità dell'impatto (es. danni finanziari, discriminazione, perdita di controllo su dati sensibili) sia la probabilità che quel danno si concretizzi; solo se entrambe le componenti indicano un rischio non trascurabile, la notifica è necessaria.

Anche quando il titolare decide di non notificare perché ritiene che il rischio sia trascurabile o "nullo", deve registrare l'incidente, le misure adottate e le motivazioni della decisione, anche in forma sintetica.

Lo schema di valutazione del rischio è riportato nelle due tabelle che seguono: la prima definisce i livelli di Probabilità (1–5) in termini di concretizzazione del danno alla privacy; la seconda definisce i livelli di Impatto (1–5) sulla gravità delle conseguenze per gli interessati. La soglia operativa per l'attivazione della notifica all'autorità è definita separatamente e si applica ai punteggi risultanti dall'incrocio di queste due scale. Entrambe si basano su quanto disposto dal Regolamento (UE) 2016/679 (artt. 33–34), dalle linee guida EDPB sul trattamento delle violazioni dei dati personali e dalle indicazioni operative del Garante per la protezione dei dati; per l'approccio metodologico si è altresì fatto riferimento a best practice e strumenti tecnico-operativi proposti da ENISA.

Probabilità

Livello	Descrizione sintetica	Esempio concreto
1 Molto bassa	Quasi impossibile che si verifichi un danno	È improbabile che dall'evento derivi qualsiasi danno per la privacy; i dati esposti sono non identificativi o già pubblici, o esistono barriere tecniche/organizzative che rendono la materializzazione del danno fortemente improbabile. Esempio: esportazione/copia di dati contenente solo dati già pubblici; dati cifrati con chiavi non compromesse e nessun segno di esfiltrazione delle chiavi.
2 Bassa	Possibile, ma improbabile che succeda qualcosa di rilevante	Esiste una minima possibilità che l'evento porti a un danno per la privacy; servirebbero ulteriori azioni ed elementi perché il danno si realizzi. Esempio: esposizione temporanea di indirizzi email aziendali; dati parziali che da soli non consentono furto d'identità.
3 Moderata	Plausibile in certe condizioni	È plausibile che, con uno sforzo limitato o combinando informazioni, l'evento possa tradursi in danno per gli

		interessati; il contesto o il tipo di dato aumenta la possibilità concreta di impatto. Esempio: elenco di nomi con codici fiscali parziali.
4 Alta	Probabile che si verifichi un danno	È probabile che l'evento causi danno per la privacy senza necessità di interventi complessi; i dati esposti sono sufficienti per frodi, furto d'identità o altri pregiudizi. Esempio: esposizione di dati bancari parziali collegabili a soggetti specifici.
5 Molto alta	Danno quasi certo o già in corso	È quasi certo che si sia verificato o si verificherà un danno per la privacy; esistono prove di uso improprio, diffusione pubblica o compromissione delle chiavi/credenziali che rendono il danno imminente o già in atto. Esempio: dati sensibili resi pubblici su forum; credenziali compromesse; evidenza di esfiltrazione e vendita dei dati.

Impatto

Livello	Descrizione sintetica	Esempio concreto
1 Trascurabile	Nessuna conseguenza pratica per le persone	Nessuna conseguenza prevedibile per la privacy. I dati compromessi non permettono identificazione o abuso. Esempio: file contenente solo dati già pubblici o anonimizzati in modo irreversibile.
2 Basso	Conseguenze limitate, facilmente risolvibili	Rischio di disagio minimo, piccoli inconvenienti, conseguenze marginali. Esempio: esposizione di indirizzi email aziendali pubblici; nomi senza ulteriori identificatori.
3 Moderato	Danno rilevabile ma non grave o duraturo	Gli interessati possono incontrare alcuni disagi, che dovrebbero essere in grado di superare nonostante alcune difficoltà. Può richiedere azioni correttive dagli interessati. Rischio di frode o danno reputazionale limitato. Esempio: numeri di telefono, identificativi parziali, o dataset che permettono phishing mirato se combinati con altre fonti.
4 Alto	Danno significativo o perdite economiche	Gli individui possono incontrare significativi disagi, che dovrebbero essere in grado di superare anche se con gravi difficoltà. Dati bancari parziali; informazioni che permettono furto d'identità

5 Critico	Danno grave, duraturo o per la sicurezza delle persone	Dati sanitari sensibili, informazioni di sicurezza nazionale, rischio per l'incolumità

Terminate le valutazioni di Probabilità e Impatto, si passa a calcolare la somma P + I e si applica la soglia operativa descritta nella sezione seguente per determinare se procedere con la notifica all'autorità e/o con la comunicazione agli interessati, in conformità al seguente modello:

- se P + I ≥ 8 → notifica all'autorità e si valuta anche la eventuale comunicazione agli interessati;
- se P + I = 7 → valutazione prudenziale: se Impatto ≥ 4 o ci sono elementi di incertezza, preferire la notifica; altrimenti documentare la decisione e monitorare;
- se P + I ≤ 6 → di norma non notificare; registrare l'incidente, le evidenze e le misure adottate; riesaminare se emergono nuovi elementi.

Gli aspetti sopra citati andranno comunque soppesati e potrebbero condurre, quale regola prudenziale, alla notifica anche con somma < 8. Ad esempio, in tutti i casi in cui esistono evidenze di uso improprio o diffusione dei dati (es. dati pubblicati online, vendita, frodi già avvenute).

10.2 Fase 4 – Raccolta informazioni e invio notifica al Garante

Nel caso di Data Breach, qualora la valutazione abbia condotto a concludere che non sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, occorre notificare al Garante la violazione. La notifica deve contenere almeno gli elementi riportati nell'art. 33 del GDPR, e deve essere eventualmente corredata da una motivazione per il ritardo se effettuata oltre le 72h dal momento in cui il Titolare o i delegati all'attuazione del trattamento sono venuti a conoscenza della violazione di sicurezza.

Tra gli elementi devono essere forniti almeno (cfr. art 33 GDPR):

- natura della violazione;
- nome e dati di contatto del Responsabile della protezione dei dati o altro punto di contatto;
- probabili conseguenze della violazione dei dati personali;
- misure adottate o di cui si propone l'adozione per rimediare alla violazione.

10.3 Fase 5 - Comunicazione agli interessati

Nel caso in cui la valutazione del rischio effettuata in precedenza risulti elevata e non si incorra in una delle clausole che sollevano il Titolare dalla necessità di effettuare la comunicazione (cfr. art. 34 GDPR), occorre predisporre una comunicazione agli interessati a cui i dati violati si riferiscono. La comunicazione deve contenere almeno:

- il nome e i dati di contatto del Responsabile della protezione dei dati o i riferimenti di un contatto alternativo per ottenere informazioni ulteriori;
- le probabili conseguenze della violazione;
- le misure adottate per porre rimedio alla violazione.

10.4 Fase 6 - Registrazione del data breach

La violazione dei dati personali, sia essa soggetta o meno alla notifica all'Autorità garante, viene registrata nel Registro delle violazioni. Per ogni registrazione sono riportati:

- le cause della violazione;
- la descrizione di ciò che è avvenuto;
- i dati personali interessati dalla violazione;

- le azioni correttive adottate;
- le valutazioni fatte laddove si sia deciso di non notificare il data breach all'Autorità di controllo o di non comunicare la violazione agli interessati;
- se del caso, i motivi del ritardo della notifica all'Autorità.

11 Matrici RACI – Ruoli e responsabilità

Per la chiara attribuzione delle responsabilità nelle attività di gestione degli incidenti informatici (inclusi i data breach), l'Ente adotta una matrice RACI, che definisce per ciascuna attività i ruoli coinvolti secondo le seguenti categorie:

R – Responsible (Responsabile operativo)

Soggetto o funzione che esegue operativamente l'attività o il compito assegnato. Possono essere presenti più soggetti "R" per la stessa attività, qualora la sua esecuzione richieda il coinvolgimento di più unità.

A – Accountable (Responsabile ultimo)

Soggetto o funzione che ha la responsabilità finale dell'attività e del suo esito, nonché del rispetto delle tempistiche e delle decisioni correlate. Per ciascuna attività è individuato un solo "A", al fine di evitare sovrapposizioni o incertezze.

C – Consulted (Consultato)

Soggetto o funzione che deve essere coinvolto preventivamente rispetto allo svolgimento dell'attività o all'adozione di decisioni rilevanti. Fornisce pareri, competenze specialistiche e validazioni. Il flusso informativo è bidirezionale (confronto e scambio di informazioni).

I – Informed (Informato)

Soggetto o funzione che deve essere tenuto informato sull'avvio, lo stato di avanzamento o l'esito dell'attività, senza partecipare direttamente all'esecuzione o al processo decisionale.

Nel presente Piano sono definite **tre matrici RACI distinte**, applicate alle fasi del processo come segue:

1. **matrice RACI per gli incidenti di sicurezza informatica**, articolata nelle seguenti fasi:
    - Rilevazione e Segnalazione;
    - Classificazione e Analisi;
    - Contenimento e Mitigazione;
    - Comunicazione e Notifica;
    - Risoluzione e Ripristino;
    - Reporting e Miglioramento.
2. **due matrici RACI specifiche per i data breach**, entrambe riferite alle seguenti fasi (le prime due fasi coincidono con quelle previste per gli incidenti di sicurezza informatica):
    - Rilevazione e Segnalazione;
    - Classificazione e Analisi;
    - Valutazione;
    - Raccolta informazioni e invio al Garante;
    - Comunicazione interessati e riscontri;
    - Registrazione della violazione.

Le tre matrici sono predisposte per garantire una chiara separazione e tracciabilità delle responsabilità tra la gestione degli incidenti di sicurezza informatica in generale e la gestione delle violazioni di dati personali, in particolare con riferimento agli obblighi di notifica al Garante e di comunicazione agli interessati.

11.1 Figure coinvolte

Le figure coinvolte sono descritte nel paragrafo 6 “Ruoli e responsabilità: il Presidio per la cybersicurezza e la protezione dei dati del Consiglio regionale”.

La composizione del **Presidio per la cybersicurezza e la protezione dei dati** è la seguente:

- Segretaria Generale e Direttore con competenza in materia di transizione al digitale;
- Direttore e Dirigente responsabile della struttura organizzativa nella quale si verifica l’incidente e/o la violazione dei dati;
- Responsabile sistemi informativi (coincide con il ruolo di CISO, Responsabile sicurezza delle informazioni);
- Responsabile protezione dati personali (DPO).

11.2 Matrice RACI Gestione incidenti di cybersicurezza

Fase	Responsible (R)	Accountable (A)	Consulted (C)	Informed (I)
Rilevazione e Segnalazione	Settore Sistemi informativi, D-SOC CSI Piemonte, Presidi CSI in CRP	CISO	D-SOC CSI Piemonte, DPO	Presidio cybersicurezza
Classificazione e Analisi	Settore Sistemi informativi, Presidi CSI in CRP	CISO	D-SOC CSI Piemonte, DPO	Presidio cybersicurezza
Contenimento e Mitigazione	Settore Sistemi informativi, D-SOC CSI Piemonte, Presidi CSI in CRP	CISO	D-SOC CSI Piemonte, DPO	Presidio cybersicurezza
Comunicazione e Notifica	Punto di contatto / Referente CSIRT	CISO	Presidio cybersicurezza	Autorità, stakeholder, CISO CSI Piemonte
Risoluzione e Ripristino	Settore Sistemi informativi, D-SOC CSI Piemonte, Presidi CSI in CRP	CISO	Presidio cybersicurezza	Presidio cybersicurezza
Reporting e Miglioramento	Settore Sistemi informativi	CISO		Presidio cybersicurezza

11.3 Matrice RACI Gestione data breach – violazione su archivio informatico

Nel caso in cui l'incidente sia qualificabile come Data Breach, oltre al Presidio sopra illustrato, sono coinvolte anche le figure del Titolare, del Responsabile della gestione documentale, la Coordinatrice, la Segretaria e i componenti del Gruppo dei referenti privacy di settore.

Fase	Responsabile (R)	Accountable (A)	Consulted (C)	Informed (I)
Rilevazione e Segnalazione	Segr. Generale, Direttori e Dirigenti delegati	CISO	DPO	
Classificazione e Analisi	Settore Sistemi informativi, Presidi CSI in CRP	CISO	D-SOC CSI Piemonte, DPO	Presidio cybersicurezza
Valutazione	Presidio cybersicurezza	Segr. Generale, Direttori e Dirigenti delegati	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria)	
Raccolta informazioni e invio al Garante	Segr. Generale, Direttori e Dirigenti delegati	Titolare / Cotitolare del trattamento	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria), CISO	Resp. Gest. doc, Garanti (se coinvolti)
Comunicazione interessati e riscontri	Segr. Generale, Direttori e Dirigenti delegati	Titolare / Cotitolare del trattamento	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria)	Soggetti interessati dalla violazione, Resp. Gest. doc, Garanti (se coinvolti)
Registrazione della violazione	Settore Sistemi informativi	Segr. Generale, Direttori e Dirigenti delegati	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria), CISO	Presidio cybersicurezza, Resp. Gest. doc.

11.4 Matrice RACI Gestione data breach – violazione su archivio cartaceo

Nel caso in cui l'incidente sia qualificabile come Data Breach, oltre al Presidio sopra illustrato, sono coinvolte anche le figure del Titolare, del Responsabile della gestione documentale, la Coordinatrice, la Segretaria e i componenti del Gruppo dei referenti privacy di settore.

Fase	Responsabile (R)	Accountable (A)	Consulted (C)	Informed (I)
Rilevazione e Segnalazione	Resp. Gest. doc.	Segr. Generale, Direttori e Dirigenti delegati	DPO	CISO

Classificazione e Analisi	Resp. Gest. doc.	Segr. Generale, Direttori e Dirigenti delegati	D-SOC CSI Piemonte, DPO, CISO	Presidio cybersicurezza
Valutazione	Resp. Gest. doc., Presidio cybersicurezza	Segr. Generale, Direttori e Dirigenti delegati	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria)	
Raccolta informazioni e invio al Garante	Segr. Generale, Direttori e Dirigenti delegati	Titolare/Cotitolare del trattamento	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria), Resp. Gest. doc.	Garanti (se coinvolti), CISO
Comunicazione interessati e riscontri	Segr. Generale, Direttori e Dirigenti delegati	Titolare / Cotitolare del trattamento	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria)	Soggetti interessati dalla violazione, Garanti (se coinvolti)
Registrazione della violazione	Settore Sistemi informativi	Segr. Generale, Direttori e Dirigenti delegati	DPO, Tavolo referenti privacy (componenti, coordinatrice e segretaria), CISO	Presidio cybersicurezza, Resp. Gest. doc.

12 Gli incidenti significativi in materia di cybersicurezza e i data breach

L'articolo 25 del d.lgs. n. 138 del 2024 impone sia ai soggetti qualificati "essenziali" sia a quelli "importanti" l'obbligo di notificare ogni incidente che ha un impatto significativo sulla fornitura dei loro servizi. La notifica dev'essere effettuata al CSIRT che è entità, all'interno dell'Agenzia per la cybersicurezza nazionale (ACN), che si occupa di prevenire, analizzare e rispondere agli incidenti di sicurezza informatica.

Un incidente è significativo se:

- ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;
- ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

L'allegato 3 della determinazione del Direttore Generale dell'Agenzia per la cybersicurezza nazionale del 14 aprile 2025, n. 164179, individua anche le tipologie di incidenti significativi secondo il seguente schema.

Codice	**Descrizione**
IS-1	Il soggetto NIS ha evidenza della perdita di riservatezza, verso l'esterno, di dati digitali di sua proprietà o sui quali esercita il controllo, anche parziale.
IS-2	Il soggetto NIS ha evidenza della perdita di integrità, con impatto verso l'esterno, di dati di sua proprietà o sui quali esercita il controllo, anche parziale.

IS-3	Il soggetto NIS ha evidenza della violazione dei livelli di servizio attesi dei suoi servizi e/o delle sue attività, sulla base dei livelli di servizio atteso (SL) definiti ai sensi della misura DE.CM-01.

Per "Data Breach" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Con questo termine ci si riferisce ad un incidente di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

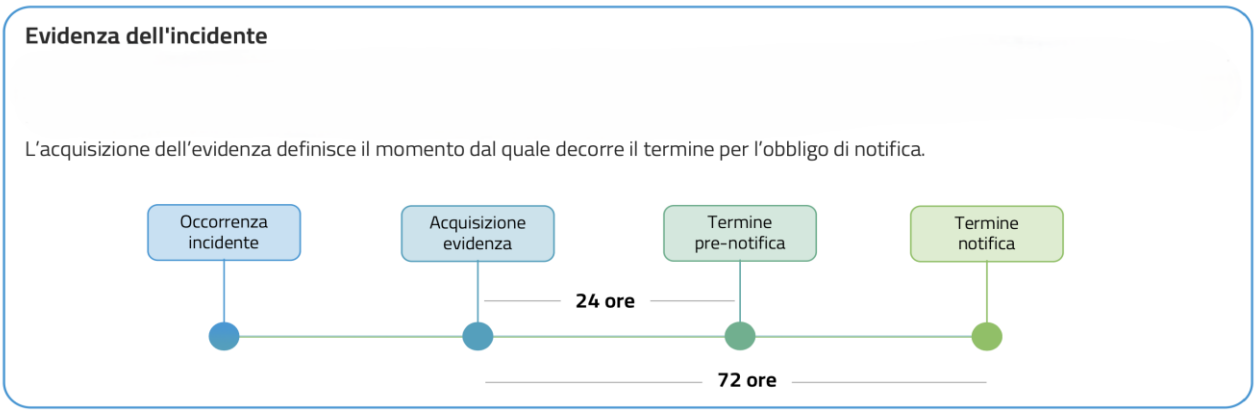
13 Notifiche verso autorità e organismi nazionali

L'articolo 25 del decreto NIS stabilisce anche che i soggetti interessati trasmettano al CSIRT la segnalazione degli incidenti significativi con le seguenti modalità e tempistiche:

- entro 24 ore, pre-notifica (segnalazione) che, ove possibile, indichi se l'incidente possa ritenersi il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero;
- entro 72 ore, notifica che, ove possibile, aggiorni le informazioni della pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;
- su richiesta del CSIRT, relazione intermedia con aggiornamenti sulla situazione;
- entro 30 giorni, relazione finale che comprenda:
  - una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
  - il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
  - le misure di attenuazione adottate e in corso;
  - ove noto, l'impatto transfrontaliero dell'incidente.

Se l'incidente è ancora in corso dopo 30 giorni, una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Il termine per l'obbligo di notifica decorre dal momento in cui è acquisita l'evidenza dell'incidente come raffigurato nella figura seguente.



L'art. 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali entro settantadue ore dal momento in cui il titolare ne viene a conoscenza.

Si è "a conoscenza" di una violazione nel momento in cui si accerta che la violazione è avvenuta e il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione (Gruppo WP 29 – Linee guida sulla notifica delle violazioni di dati personali del 6 febbraio 2018).

Di conseguenza, il termine per la notifica al Garante decorre nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Il termine delle settantadue ore non è perentorio, tuttavia, nel caso in cui questo termine sia superato, unitamente alla notifica, occorre giustificare i motivi del ritardo (art. 33 paragrafo 1 del GDPR).

Secondo il sopracitato articolo 33 la notifica al Garante non è necessaria quando sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Come sarà esposto nella fase relativa alla "Valutazione", le violazioni di dati personali devono essere notificate all'autorità di controllo quando, a seguito della violazione, sussiste un rischio elevato per i diritti e le libertà delle persone fisiche. Non è richiesto che il danno sia già occorso: è sufficiente una probabilità significativa che possano concretizzarsi effetti avversi rilevanti.

Per "effetti avversi rilevanti" si intendono, a titolo esemplificativo, la perdita del controllo sui propri dati personali, la limitazione di diritti, la discriminazione, il furto di identità, il rischio di frode, la perdita di riservatezza di informazioni protette dal segreto professionale, una perdita finanziaria, un danno alla reputazione o qualsiasi altro significativo svantaggio economico o sociale.

La presenza di uno degli effetti sopra elencati non determina automaticamente l'obbligo di notifica: l'obbligo scatta solo dopo una valutazione concreta e documentata di probabilità e gravità. Se la valutazione conclude che il rischio è basso o trascurabile, il titolare non è tenuto a notificare, ma deve comunque registrare l'incidente, motivare la decisione e conservare le evidenze e le misure di mitigazione adottate.

14 Comunicazione interna

La segnalazione di un potenziale incidente o di una violazione dei dati personali può essere effettuata da qualsiasi soggetto interno o esterno del Consiglio regionale attraverso i canali previsti dalle procedure operative.

Le comunicazioni interne seguono il principio del need-to-know e sono indirizzate al CISO, quale referente centrale per la gestione degli incidenti di sicurezza informatica, al DPO, quale referente per la gestione delle violazioni, al Presidio per la cybersicurezza del Consiglio regionale. Le procedure operative indicano le modalità e i flussi da seguire.

15 Comunicazione pubblica e relazioni esterne

Nel caso di incidenti di particolare rilevanza pubblica o potenziale impatto reputazionale, il Presidio per la cybersicurezza definisce le modalità e i contenuti delle comunicazioni esterne, nel rispetto delle normative sulla trasparenza e sulla sicurezza nazionale.

Le comunicazioni verso media, organi di stampa o altri organi di comunicazione esterni sono effettuate esclusivamente attraverso i canali ufficiali del Consiglio regionale.

Nel caso in cui l'Agenzia per la Cybersicurezza Nazionale (ACN), ai sensi dell'art. 37, comma 3, lettera i) del decreto NIS, intimasse all'Ente di informare il pubblico riguardo a un incidente informatico, quest'ultimo adotta un processo strutturato per garantire una comunicazione tempestiva, trasparente e coerente.

La ricezione dell'intimazione da parte dell'ACN attiva tempestivamente il Presidio per la cybersicurezza. Questo gruppo ha il compito di raccogliere le informazioni necessarie e predisporre un comunicato ufficiale da diffondere al pubblico.

Il comunicato viene redatto seguendo alcuni principi fondamentali:

- trasparenza, per assicurare che le informazioni siano accurate e comprensibili;

- tempestività, per rispettare le scadenze indicate dall'ACN;
- coerenza, affinché i messaggi diffusi attraverso i diversi canali (sito web, social media, comunicati stampa) siano uniformi;
- tutela, per evitare la divulgazione di dati sensibili o di dettagli tecnici che possano compromettere ulteriormente la sicurezza.

Il testo del comunicato, validato e approvato dal Presidio per la cybersicurezza, contiene una descrizione sintetica dell'incidente, l'indicazione dell'impatto sugli utenti o cittadini, le misure adottate per mitigare le conseguenze e, ove necessario, istruzioni pratiche per ridurre i rischi (ad esempio, modificare le credenziali o prestare attenzione a possibili campagne di phishing).

16 Tracciabilità e riservatezza

Tutte le comunicazioni e notifiche relative agli incidenti di cybersicurezza e ai data breach sono tracciate e archiviate in modo sicuro, nel rispetto delle politiche di conservazione dei dati e della gestione documentale del Consiglio regionale.

L'accesso alle informazioni è limitato ai soli soggetti autorizzati, nel rispetto del principio di minimizzazione e dei requisiti di integrità e riservatezza delle informazioni.

17 Diffusione e consapevolezza

Il Piano di gestione degli incidenti di sicurezza è pubblicato sul portale intranet del Consiglio regionale e reso disponibile a tutto il personale e ai soggetti interessati.

CONSIGLIO REGIONALE DEL PIEMONTE

Istruzioni operative ai sensi dell'articolo 32 del GDPR per l'utilizzo dei dispositivi informatici, dei servizi digitali e della gestione documentale nell'attività lavorativa. Disciplinare interno.

Dicembre 2025

Sommario

Adozione del disciplinare e sua efficacia

Il Disciplinare è stato redatto da apposito gruppo di lavoro inter-direzionale e approvato con Deliberazione dell'UdP n. 273 del 28/12/2018 nella sua prima versione.

A giugno 2021 si rese necessario un aggiornamento, approvato con Deliberazione dell'UdP n. 101 del 17 giugno 2021, a seguito dell'introduzione di nuovi servizi informatici di supporto alle attività dell'Assemblea regionale e delle direzioni del Consiglio (sistemi di videoconferenza e remotizzazione delle postazioni di lavoro).

A maggio 2024 si è reso necessario un ulteriore aggiornamento, approvato con Deliberazione dell'UdP n. 108 del 23/05/2024, per recepire quanto previsto dal DPR 13 giugno 2023 all'art. 11-bis rubricato "Utilizzo delle tecnologie informatiche" (modifica al DPR 16 aprile 2013 recante il codice di comportamento dei

dipendenti pubblici). Si esplicitano inoltre i tempi di conservazione dei log di sistema, come da indicazioni del Garante Privacy, e si introduce un nuovo paragrafo dedicato agli strumenti di intelligenza artificiale.

A dicembre 2025 si è reso necessario un ulteriore aggiornamento per coordinare le istruzioni operative con il Piano di gestione degli incidenti di cybersicurezza e dei data breach (art. 25 d.lgs. 138/2024, artt. 32-33-34 GDPR)

I dipendenti del Consiglio regionale del Piemonte saranno informati tramite apposita circolare e il Disciplinare sarà reso disponibile anche sulla intranet.

Il Disciplinare potrà essere aggiornato ogni qualvolta se ne presenti l'opportunità e di tali revisioni sarà data tempestiva comunicazione ai dipendenti.

Le disposizioni contenute nel Disciplinare si applicano a tutto il personale del Consiglio regionale del Piemonte, nonché a tutti i soggetti che utilizzano strumenti informatici e servizi digitali o documentali del Consiglio (in particolare, garanti, Corecom, gruppi consiliari, uffici di comunicazione, borsisti, consulenti, tecnici in presidio). Le disposizioni sono rivolte a chiunque effettui trattamento di dati personali, anche nell'ambito di progetti didattici e per periodi limitati di tempo.

È responsabilità di chiunque applicare e rispettare puntualmente le disposizioni del presente Disciplinare.

Il contenuto del presente documento costituisce ordine di servizio, pertanto la mancata ottemperanza a quanto disposto nel presente documento integra, oltre ad eventuali altri profili di responsabilità civile, penale ed erariale, anche un'ipotesi di violazione disciplinare.

Riferimenti normativi

- Codice dell'Amministrazione Digitale D. Lgs. 82/2005 e s.m.i.;
- Regolamento UE 679/2016 (GDPR- General Data Protection Regulation), di seguito "GDPR", decreto legislativo 196/2003, così come modificato e integrato dal decreto legislativo 101/2018;
- DPR n. 62 del 16 aprile 2013 Codice di comportamento dei dipendenti pubblici, modificato dal DPR n. 81 del 13 giugno 2023;
- DUP n. 113 del 22 maggio 2018;
- DUP n. 185 del 17 dicembre 2020;
- DUP n. 49 del 25 marzo 2021;
- Direttiva (UE) 2022/2555 nota come "Direttiva NIS2";
- Legge 90/2024 Disposizioni in materia di cybersicurezza per le pubbliche amministrazioni e i soggetti pubblici e privati operanti in settori strategici;
- D.Lgs. 138/2024 noto come "Decreto NIS";
- DUP n. 189 del 23 luglio 2025 Adempimenti reg. UE 679/2016;
- DUP n. 318 del 18 dicembre 2025 di approvazione del Piano generale di attuazione della direttiva (UE) 2022/2555 "NIS 2" e del d.lgs. 138/2024 in Consiglio regionale del Piemonte.
- DUP n. 319 del 18 dicembre 2025 di approvazione del Piano di gestione degli incidenti di cybersicurezza (art. 25 D.lgs. 138/2024) e delle violazioni di dati personali (data breach - artt. 33 e 34 Reg. (UE) 2016/679)

Principi generali

Il Disciplinare è adottato per assicurare la funzionalità e il corretto impiego dei personal computer portatili o fissi, dei dispositivi elettronici aziendali in generale, della posta elettronica, di internet e di tutti i servizi

digitali da parte del personale: a tale fine, definisce le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali.

Le disposizioni e le prescrizioni qui indicate si affiancano e integrano quelle già previste nel contratto di lavoro e, in generale, nelle disposizioni pattizie o regolamentari vigenti.

L'osservanza delle presenti disposizioni, oltre a garantire il corretto trattamento dei dati personali, costituisce una misura organizzativa essenziale per la sicurezza dei sistemi informativi e di rete del Consiglio regionale, contribuendo alla prevenzione, alla tempestiva rilevazione e alla gestione degli incidenti di cybersicurezza in coerenza con il Piano di gestione degli incidenti di cybersicurezza e dei data breach.

Le regole che disciplinano l'utilizzo del personal computer, dei dispositivi elettronici aziendali, della posta elettronica, di internet e di tutti i servizi digitali si conformano, inoltre, ai principi generali sanciti dal Regolamento Europeo 679/2016 e dal decreto legislativo 196/2003, così come modificato e integrato dal decreto legislativo 101/2018:

a) «liceità, correttezza e trasparenza». Liceità indica che ogni trattamento deve trovare fondamento in un'idonea base giuridica. I fondamenti di liceità del trattamento di dati personali sono indicati all'articolo 6 del GDPR: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

Correttezza allude alla lealtà e alla buona fede che il titolare deve osservare in tutte le fasi del trattamento dei dati.

Trasparenza significa invece garantire la piena consapevolezza all'interessato circa il soggetto che tratta i suoi dati e le modalità con cui li tratta. Lo strumento per dare attuazione a tale principio è l'informativa: l'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato, sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento.

b) «limitazione della finalità»: i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) «minimizzazione dei dati»: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) «esattezza»: i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;

e) «limitazione della conservazione»: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato;

f) «integrità e riservatezza»: i dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali).

CONSIGLIO REGIONALE DEL PIEMONTE

Disposizioni relative all'utilizzo dei dispositivi informatici

I dispositivi informatici costituiscono la postazione di lavoro degli utenti dei servizi digitali del Consiglio, sono rappresentati da personal computer portatili o fissi, tablet e smartphone, e dai programmi su di essi installati: le postazioni sono strumenti di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla privacy.

Vanno pertanto utilizzati e conservati con diligenza e cura, attenendosi alle prescrizioni fornite dal datore di lavoro e nel rispetto delle indicazioni da questo fornite.

Le impostazioni delle postazioni informatiche e dei relativi programmi installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dall'Amministrazione consiliare, in funzione della qualifica dell'utente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Amministrazione consiliare stessa. L'utente non può modificarle autonomamente: può ottenere cambiamenti nelle impostazioni solo previa richiesta del Direttore della struttura di appartenenza al Settore Sistemi Informativi.

L'installazione sulle postazioni informatiche di sistemi operativi e programmi applicativi e, in generale, di software, avviene ad opera dei tecnici informatici incaricati, che operano seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate.

L'installazione di programmi da parte dell'utente non è consentita: in caso di necessità occorre rivolgersi, previa autorizzazione del proprio Direttore, al Settore Sistemi Informativi. In ogni caso tale installazione deve avvenire senza aggirare divieti o restrizioni che disciplinano l'utilizzo di tali programmi e, in generale, della normativa vigente, con particolare riferimento alle disposizioni in materia di protezione di diritti di proprietà intellettuale: abusi o utilizzi illeciti saranno puniti conformemente alle disposizioni che disciplinano il rapporto di lavoro.

Tutti i software caricati sulle postazioni informatiche ed in particolare i software necessari per la protezione dello stesso o della rete, non possono essere disinstallati o in nessun modo manomessi dagli utenti.

I privilegi di amministratore non sono attribuibili agli utenti, per ragioni di sicurezza. L'attribuzione temporanea di tali privilegi può essere effettuata solo per casi eccezionali, da valutarsi puntualmente rispetto al rischio e da autorizzarsi in forma scritta dal responsabile di direzione. Deve esserne tenuto un registro, nel quale ci sia evidenza delle operazioni effettuate.

L'accesso alle postazioni informatiche, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento dell'attività avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di credenziali identificative nonché, quando richiesto dal sistema, di un certificato digitale.

Scelta, custodia, modifica e utilizzo delle password devono rispettare le seguenti prescrizioni:

- Al primo accesso ad un sistema e/o ad una banca dati, l'utente ha la responsabilità di cambiare la password assegnatagli;
- La password deve essere al minimo lunga otto caratteri, deve contenere una combinazione di lettere, numeri e caratteri speciali, deve essere differente dalle tre precedenti usate e non deve contenere riferimenti che possano ricondurre agevolmente al responsabile della stessa;
- L'utente è obbligato dal sistema a cambiare la propria password su base almeno trimestrale;
- L'utente ha la responsabilità di custodire con diligenza la propria password (ed i dispositivi fisici eventualmente in suo possesso). In nessuna circostanza l'utente è autorizzato a condividere le proprie credenziali di autenticazione con altri incaricati o terze persone.
- Analogamente non possono essere richieste attribuzioni di credenziali o reset di pw per soggetti terzi.

- Se le credenziali sono state create dai servizi di assistenza, devono essere obbligatoriamente modificate al primo utilizzo, e mai salvate automaticamente per i successivi utilizzi delle applicazioni.

Sono fatte salve tutte le prescrizioni ulteriori previste per il trattamento dei dati particolari o giudiziari.

In caso di furto o smarrimento delle credenziali, o comunque in tutti i casi in cui l'utente abbia fondati motivi di ritenere che ne possa essere stato fatto un utilizzo da parte di terzi, l'utente deve darne immediatamente informazione all'Amministrazione consiliare con contestuale denuncia all'autorità competente. Nel caso in cui l'utente abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito, deve attenersi alla procedura di segnalazione approvata dal direttore competente in materia di sistemi informativi e transizione digitale.

In caso di allontanamento anche temporaneo dalla postazione informatica, l'utente deve evitare che persone estranee effettuino accessi non permessi, bloccandola.

Al termine della giornata di lavorativa o in caso di allontanamento prolungato dalla postazione di lavoro, i dispositivi assegnati lasciati in ufficio devono essere riposti in cassetti o armadi chiusi a chiave.

Le credenziali di accesso degli utenti saranno disattivate nel caso in cui cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa.

Qualora sia necessario accedere a informazioni o documenti di lavoro presenti sulla postazione informatica del dipendente assente e unicamente per garantire l'operatività aziendale, il Direttore della struttura di appartenenza chiede per iscritto al Settore Sistemi Informativi di essere messo nelle condizioni di accedere alla postazione informatica stessa. Contestualmente, il Direttore deve informare il dipendente dell'avvenuto accesso, fornendo adeguata spiegazione e redigendo apposito verbale.

Per finalità di manutenzione e aggiornamento, gli incaricati del Settore Sistemi Informativi potranno accedere sia direttamente sia in remoto alla postazione informatica in via generalizzata. Resta inteso che per finalità di assistenza tali soggetti potranno accedere sia direttamente sia in remoto su richiesta del dipendente.

Dispositivi mobili

Particolare attenzione va posta verso i dispositivi mobili, per loro natura estremamente vulnerabili, sono veri e propri punti di accesso al sistema informativo del Consiglio; è fondamentale proteggerne l'accesso mediante gli strumenti messi a disposizione dal loro sistema operativo, cambiando regolarmente i codici.

La stessa cura deve essere prestata su dispositivi mobili personali sui quali siano possibili accessi a servizi digitali del Consiglio (es. la posta elettronica, le rubriche, ecc.): i dispositivi devono essere protetti da codici di accesso. In caso di smarrimento, furto o di utilizzo dei dispositivi da parte di soggetti non autorizzati, occorre effettuare tempestivamente la segnalazione secondo la procedura di segnalazione approvata dal direttore competente in materia di sistemi informativi e transizione digitale (vedi paragrafo "Comportamento in caso di violazione della sicurezza").

Memorizzazione dei dati – archivi digitali

Al fine di garantire la disponibilità dei documenti di lavoro, l'utente potrà usufruire dell'area di rete individuale o di gruppo a ciò dedicata (dischi condivisi).

I supporti di memoria portatili e comunque riutilizzabili dovranno essere custoditi con la massima cura ed utilizzati adottando le necessarie cautele affinché soggetti estranei non possano venire a conoscenza dei documenti e delle informazioni ivi contenute.

Tutti i dispositivi elettronici aziendali sono forniti all'utente per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato, con esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali.

Gli utenti dei servizi digitali del Consiglio regionale devono sempre utilizzare per la memorizzazione dei dati, gli appositi share di rete messi a disposizione dall'Ente (abilitati ai soli addetti) o i relativi database previsti dai progetti. In caso di necessità (anche solo temporanea) di mantenere per fini di lavorazione una copia delle informazioni offline (sul disco interno delle postazioni di lavoro, su chiavette USB, su hard disk esterni, su smartphone, tablet, ecc.), la copia locale deve essere cifrata ed eliminata al termine della lavorazione.

Non è consentito salvare dati e informazioni su strumenti cloud di archiviazione, gratuiti o a pagamento (es. Google Drive, Dropbox, ecc.), diversi da quelli messi a disposizione dal Consiglio regionale.

Utilizzo di internet e delle risorse di rete

La rete internet può e deve essere utilizzata dal dipendente a supporto all'attività lavorativa.

Al fine di ridurre il rischio di un utilizzo improprio di internet, quale ad esempio il caricamento o lo scaricamento di documenti non attinenti con l'attività lavorativa, la visione di siti internet non pertinenti con l'attività svolta, il collegamento a reti o forum comunque estranei alle mansioni del dipendente, si ricorda che:

- occorre prestare rispetto della normativa vigente in materia di protezione di diritti di proprietà intellettuale nell'acquisizione, riproduzione, condivisione di immagini, di musica, filmati, software;
- il Consiglio regionale utilizza sistemi e filtri automatici che prevengono determinate operazioni non attinenti all'attività lavorativa, bloccando l'accesso a predeterminate categorie di siti;
- i log di connessione alla posta elettronica e di navigazione in Internet degli utenti sono conservati per finalità di accertamento e repressione dei reati nel rispetto di quanto previsto dalla normativa vigente (di seguito approfondimento).

Si ribadisce che ogni utente è tenuto ad utilizzare Internet e le risorse di rete nel pieno rispetto delle leggi vigenti.

Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

Fra le misure tecniche adottate per prevenire abusi o minacce alla sicurezza, in Consiglio è attivo il tracciamento delle attività sugli applicativi del Sistema Informativo, da/per l'esterno della rete dell'ente, degli accessi tramite la VPN e la conservazione dei log di traffico telematico, per le seguenti finalità: per ragioni di sicurezza interna, statistiche, prevenzione/ accertamento di illeciti e reati, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta da parte della medesima. I log vengono conservati per il tempo strettamente necessario al perseguimento delle finalità su indicate. Il tempo di conservazione stabilito dall'ente per questa tipologia di log è di 7 giorni.

Utilizzo della posta elettronica

La casella di posta elettronica istituzionale è uno strumento finalizzato esclusivamente allo scambio di informazioni nell'ambito dell'attività lavorativa.

Le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente. I messaggi di posta elettronica devono contenere un avvertimento ai destinatari del seguente tenore letterale:

"Il presente messaggio, corredato degli eventuali allegati, contiene informazioni da considerarsi strettamente riservate e confidenziali. Ne è vietato l'uso improprio, la diffusione, la distribuzione o la

riproduzione da parte di altre persone e/o entità diverse da quelle specificate. Qualora lo abbiate ricevuto per errore, vi preghiamo di distruggere il messaggio, comunicando l'errata ricezione tramite il reply all'indirizzo mittente."

Il dipendente è responsabile del contenuto dei messaggi inviati e si uniforma alle modalità di firma dei messaggi di posta elettronica di servizio.

È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

Al fine di garantire continuità e accesso ai messaggi da parte dei soggetti autorizzati a condividere tali informazioni, si raccomanda l'utilizzo di caselle di posta elettronica istituzionali in comune, eventualmente affiancandole a quelle individuali. Anche per le caselle di uso comune è necessario uniformarsi alle modalità di firma.

Qualora sia necessario accedere a informazioni o documenti di lavoro presenti nella casella di posta elettronica del dipendente assente e unicamente per garantire l'operatività aziendale, il dipendente stesso può indicare e delegare un altro lavoratore (fiduciario) a verificare il contenuto dei messaggi ed a inoltrare al Direttore della struttura di appartenenza quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In caso di assenza del fiduciario o di impossibilità di nomina dello stesso il Direttore deve chiedere per iscritto al Settore Sistemi Informativi, di essere messo nelle condizioni di accedere alla casella di posta elettronica in questione. Contestualmente, il Direttore deve informare il dipendente dell'avvenuto accesso, fornendo adeguata spiegazione e redigendo apposito verbale.

Nel caso in cui il dipendente non presti più la sua attività lavorativa presso il Consiglio regionale del Piemonte, la casella di posta elettronica sarà prontamente disattivata.

Qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura dell'utente informare prontamente il Settore Sistemi Informativi.

Gli utenti dei servizi di posta elettronica e certificata sono tenuti ad adottare gli accorgimenti di seguito indicati, per garantire la riservatezza di eventuali comunicazioni personali, la continuità operativa dell'ente nonché l'eventuale esigenza giudiziaria di verifica che renda necessaria l'apertura dello strumento di posta:

- Se si ricevono mail da destinatari sconosciuti contenenti link o allegati sospetti occorre procedere alla segnalazione al settore Sistemi Informativi ed evitarne l'apertura, sino a completa verifica.
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
- Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a queste indicazioni:
    - L'elenco dei destinatari deve essere digitato correttamente;
    - L'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile.
    - Nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.
- In caso di invio di mail a soggetti esterni, si deve evitare di mandare in chiaro l'elenco degli indirizzi dei destinatari, occorre utilizzare opportunamente la funzione di invio in copia nascosta (ccn). Gli indirizzi mail sono dati personali, non possono essere divulgati impropriamente. Elenchi di indirizzi possono facilitare lo spam e attacchi malevoli sulle caselle di posta, oltre a divulgare impropriamente i dati personali.

- Nel caso di destinatari interni è preferibile mettere in chiaro i destinatari, per competenza oppure in conoscenza (ad eccezione delle convocazioni alle sedute istituzionali, dove è consigliato mettere in ccn i destinatari).
- Occorre prestare particolare attenzione all'uso della funzione 'Inoltra' che consente di inoltrare le mail, bisogna verificare il contenuto dei messaggi inoltrati e gli indirizzi mail presenti nella cronologia del testo; un uso inappropriato dell'inoltro delle mail potrebbe infatti facilitare la divulgazione di dati personali.
- Nell'invio delle comunicazioni via mail utilizzare abitualmente le caselle di posta elettronica condivise tra più lavoratori ovvero le caselle di posta di gruppo (eventualmente affiancandole a quelle individuali).
- In caso di prolungata assenza, utilizzare le funzionalità del sistema di posta per l'invio automatico di messaggi di risposta recanti le coordinate della casella di gruppo o del proprio responsabile a cui rivolgersi.

Ai fini della sicurezza della rete dell'ente, è necessario valutare l'affidabilità del mittente prima di accedere ai file allegati alla posta elettronica (non eseguire download di file eseguibili o documenti da siti Web o Ftp ambigui o comunque non conosciuti il cui indirizzo internet è inserito nel corpo della mail).

Al fine di ridurre il rischio di diffusione di mail contenenti malware vengono applicati alla mail in ingresso filtri di controllo delle estensioni di allegati (es .zip, .rar .exe, etc) e filtri di limitazione anti-spam.

L'utilizzo di caselle di posta elettronica personali va di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore.

In Consiglio è attivo il tracciamento e conservazione dei log di posta, per le seguenti finalità: per attività di gestione del servizio (es. malfunzionamenti), per ragioni di sicurezza interna, statistiche, prevenzione/accertamento degli illeciti e reati, trasmissione dei dati all'Autorità Giudiziaria in caso di formale richiesta da parte della medesima.

Tempi di conservazione dei log del servizio di posta

I log del servizio di posta elettronica (relativi alla sola "envelope" dei messaggi ricevuti ed inviati - mittente, destinatario, data/ora - ed ai riferimenti temporali delle operazioni effettuate sulla casella - autenticazione, operazioni su mailbox, EAS, condivisioni, calendari, rubriche, conversazioni e meeting) sono conservati per un massimo di 21 gg.

I Backup dei contenuti delle caselle di posta elettronica vengono conservati per un periodo di 3 anni.

Periodo di mantenimento dei contenuti delle caselle

Le caselle di posta elettronica al momento della chiusura sono mantenute in uno stato "sospeso" (in cui non potranno essere accedute né potranno ricevere o inviare posta) per un massimo di 30 gg a decorrere dalla data di dismissione, durante i quali potrà esserne eventualmente richiesta la riattivazione (nei casi previsti dai processi interni esistenti) ripristinandone le funzionalità e il contenuto.

Trascorso tale termine, le caselle ed i rispettivi contenuti verranno cancellati definitivamente dal sistema.

Piattaforme di collaboration e video conference

Alle riunioni che si svolgono da remoto si applicano le ordinarie disposizioni sul segreto d'ufficio e sul diritto alla protezione dei dati personali.

Le piattaforme di collaboration offrono strumenti per un supporto dell'attività lavorativa a distanza sia in tempo reale (es video conferenza, condivisione e modifica di documenti tra più persone nello stesso momento) che in modalità asincrona (es. uno spazio cloud per memorizzare condividere file).

Il Consiglio regionale dispone attualmente delle piattaforme Cisco webex e Microsoft Teams, che mettono a disposizione degli utenti strumenti di videoconferenza, di condivisione in tempo reale di documenti e di messaggistica istantanea.

Gli strumenti di collaboration, quando vengono impiegati per condividere messaggi di testo, documenti, video o immagini, devono essere utilizzati nel rispetto delle regole di comportamento indicate nel disciplinare al fine di garantire la riservatezza e in generale la sicurezza delle informazioni che possono transitare sulle stesse ma anche la tutela del segreto professionale, di marchi e del know-how dell'ente.

In particolare, in relazione alla funzionalità di collaborazione in tempo reale è vietato effettuare snapshot o attivare la registrazione delle call al di fuori dei casi necessari ed espressamente autorizzati dai partecipanti.

È consentito, durante l'esecuzione delle call, l'uso delle funzioni di offuscamento delle sfondo o la disattivazione della telecamera. Le regole suindicate si applicano anche nel caso in cui vengano utilizzati strumenti di collaboration non aziendali come Skype, Zoom, Google Meet.

Tali strumenti non aziendali sono consentiti per la partecipazione a riunioni con l'esterno convocate da altri enti, ma per le riunioni interne deve essere utilizzata le piattaforme messe a disposizione dal Consiglio.

In caso di utilizzo delle videoconferenze per la gestione delle sedute istituzionali occorre attenersi al Regolamento interno del Consiglio regionale e alle norme di comportamento deliberate dall'Ufficio di Presidenza.

Strumenti di intelligenza artificiale

Premesso che gli strumenti di I.A. avranno una sempre maggiore diffusione ed utilizzo, è necessario che il personale del Consiglio ne possa fare ricorso secondo modalità efficaci, efficienti e sicure.

L'utilizzo di strumenti di IA è consentito esclusivamente quando questi siano messi a disposizione o autorizzati da parte dell'ente; tale disposizione va rispettata anche nei casi in cui l'utilizzo dello strumento di IA non richieda l'installazione di software sulla propria postazione di lavoro.

In caso di messa a disposizione o autorizzazione da parte del Consiglio di strumenti IA, è consentito solo nei casi e nelle modalità espressamente previsti:

• imputare dati/informazioni/codice di pertinenza della propria attività lavorativa all'interno di tali sistemi, inclusi dati di natura personale;

• generare materiale (es. atti, documenti, codice sorgente di software, etc…) connesso all'attività lavorativa.

Si precisa che, per finalità personali, non è possibile accedere a detti sistemi utilizzando i propri riferimenti aziendali (es: e-mail) e/o imputare dati/informazioni/codice di pertinenza della propria attività lavorativa all'interno di tali sistemi, inclusi dati di natura personale.

Disposizioni per la gestione di documenti cartacei

Per quanto riguarda la documentazione cartacea presente negli uffici occorre attenersi alle seguenti istruzioni, volte ad assicurare la protezione dei dati personali.

Stampe e fotocopie

Il Consiglio regionale ha adottato un sistema di protezione delle stampanti multifunzione, che consentono di fare scansioni, fotocopie e stampe.

Ogni utente è dotato di un codice di accesso personale, che consente di evitare improprie diffusioni di informazioni personali.

È vietato condividere con soggetti terzi il codice di accesso personale alle stampanti multifunzione.

Documenti negli uffici (scrivanie e armadi)

Per quanto riguarda l'eventuale documentazione cartacea, compresi i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati personali, soprattutto in caso di dati particolari, gli atti e i documenti dovranno essere conservati dai soggetti incaricati, esclusivamente per la durata del trattamento. Inoltre, verificare che tutti i dati raccolti siano effettivamente necessari.

Non lasciare mai documentazione sulle scrivanie oltre l'orario d'ufficio o in caso di assenza (pausa pranzo, riunione, ecc.).

Al termine del procedimento, conservare la documentazione negli archivi ad accesso selezionato e annotare il nome dei soggetti ammessi in appositi registri.

Conservare i dati idonei a rilevare lo stato di salute o in generale i dati particolari separatamente da ogni altro dato personale trattato.

Chiudere l'ufficio a chiave qualora non si abbia a disposizione un armadio munito di serratura.

Depositare le chiavi degli armadi e/o dei locali ove sono custoditi dati personali in luogo sicuro.

Effettuare la trasmissione e la comunicazione dei dati personali mediante posta, all'interno o all'esterno dell'Ente, per mezzo di supporti cartacei o magnetici, riposti in buste o pacchi chiusi. Nel caso si tratti di dati particolari, indicare sulla busta o sul pacco ovvero sul documento accompagnatorio la dicitura "dati particolari".

Comportamento in caso di violazione della sicurezza

Per incidente di cybersicurezza si intende qualsiasi evento che compromette o mette a rischio la disponibilità, l'integrità, la riservatezza o l'autenticità dei sistemi informativi, delle reti o dei servizi digitali del Consiglio regionale.

Per violazione dei dati personali (data breach) si intende, in coerenza con l'art. 4, par. 12 del GDPR, un incidente di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali, in modo accidentale o illecito.

Il data breach è quindi un particolare tipo di incidente di cybersicurezza che coinvolge dati personali.

Obbligo di segnalazione

Non appena si viene a conoscenza – o si ha un fondato sospetto – del verificarsi di un incidente di cybersicurezza o di una possibile violazione dei dati personali, al momento del fatto o della sua scoperta, il dipendente (o altro utente dei servizi informatici del Consiglio) deve segnalare l'evento senza ritardo, attenendosi alla procedura di segnalazione approvata dal direttore competente in materia di sistemi informativi e transizione digitale, che disciplina modalità e destinatari delle comunicazioni, sia per gli incidenti relativi ai sistemi e servizi informatici, sia per quelli che coinvolgono archivi cartacei.

Se la segnalazione proviene da un responsabile esterno del trattamento, da un altro ente pubblico, da fornitori, dalle forze dell'ordine, dal Garante o da altri soggetti esterni, il personale del Consiglio è tenuto a raccogliere e inoltrare la segnalazione secondo la medesima procedura.

Tutte le segnalazioni di incidenti di sicurezza e/o di data breach di cui si viene a conoscenza sono inserite nell'apposito registro gestito dalle strutture competenti, secondo le modalità stabilite dalla procedura sopra citata.

A titolo esemplificativo, devono essere segnalati come potenziali incidenti di cybersicurezza e/o data breach:

- interruzioni significative o diffuse di servizi informatici o digitali dell'Ente;
- compromissioni di fornitori o terze parti (ad esempio servizi cloud, componenti software, servizi esterni) che possano avere impatto sui sistemi del Consiglio;
- compromissioni di caselle di posta elettronica o di account utente;
- campagne di phishing o altre forme di social engineering che portino alla sottrazione o all'uso improprio di credenziali o dati;
- eventi fisici con ripercussioni sui sistemi (furti, incendi, allagamenti, danneggiamenti di locali o infrastrutture che ospitano apparati o archivi);
- uso illecito o abuso di API o di funzionalità applicative esposte verso l'esterno;
- manipolazioni dell'integrità dei dati (ad esempio alterazioni non autorizzate di database o archivi digitali);
- compromissione di infrastrutture di rete fondamentali (ad esempio sistemi DNS o instradamento di rete) o altri eventi che causino blocchi, deviazioni o uso improprio del traffico di rete;
- copia, trasferimento o estrazione non autorizzata di dati (data exfiltration);
- infezioni da malware, inclusi attacchi di tipo ransomware;
- distruzione accidentale di archivi digitali o di parti significative degli stessi;
- smarrimento o furto di PC, server o dispositivi mobili (smartphone, tablet, chiavette USB, dischi esterni, ecc.);
- smarrimento, furto o distruzione di archivi cartacei contenenti dati personali;
- divulgazione impropria di dati personali (ad esempio invio di elenchi massivi a destinatari errati o pubblicazione non autorizzata);
- indisponibilità prolungata di dati o servizi applicativi esposti su siti web o altre piattaforme digitali.

L'elenco non è esaustivo: qualsiasi evento anomalo che possa incidere sulla sicurezza dei sistemi, dei servizi o dei dati deve essere segnalato.

A fronte della segnalazione di un evento che può comportare un incidente di cybersicurezza e/o un data breach, viene attivato il Piano di gestione degli incidenti di cybersicurezza e dei data breach del Consiglio regionale del Piemonte, che disciplina le attività di analisi, mitigazione, ripristino e comunicazione verso le Autorità competenti.

Le segnalazioni raccolte attraverso la presente disciplina sono utilizzate dall'Ente anche per adempiere agli obblighi di notifica degli incidenti significativi previsti dal d.lgs. 138/2024 (attuazione della Direttiva NIS) e agli obblighi di notifica delle violazioni dei dati personali previsti dagli artt. 33 e 34 del GDPR, nel rispetto del principio del need-to-know e della riservatezza delle informazioni.

Controlli effettuati dall'Amministrazione consiliare

L'Amministrazione consiliare si riserva di effettuare controlli per verificare il rispetto del Disciplinare. Nel caso di tali controlli il presente Disciplinare costituisce preventiva e completa informazione nei confronti dei dipendenti.

Gli eventuali controlli generali ed estesi atti a verificare condotte non conformi al presente Disciplinare avverranno preliminarmente su dati aggregati e anonimi riferiti all'intera struttura lavorativa ovvero al Settore o alla Direzione qualora il Settore, per caratteristiche intrinseche alla struttura organizzativa, non offrisse garanzie di completa anonimità della verifica. Nel caso vengano rilevate anomalie o irregolarità, dovrà essere inviato un avviso generalizzato ai dipendenti che richiami questi ultimi all'utilizzo corretto degli

strumenti elettronici aziendali, nel rispetto della normativa vigente e dei diritti dei terzi, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Qualora le anomalie o le irregolarità dovessero persistere, saranno avvisate le autorità competenti.

Qualora venga constatata la violazione del presente Disciplinare, l'Amministrazione consiliare potrà irrogare le sanzioni applicabili previste dai contratti collettivi vigenti, nel rispetto delle procedure stabilite dagli stessi contratti.

L'Amministrazione consiliare effettua attività di monitoraggio e verifica dell'efficacia delle protezioni predisposte sulle postazioni informatiche rispetto ad aggressioni esterne o interne senza che siano necessarie preventive ulteriori informative. Le risultanze di tali attività di monitoraggio e verifica dovranno essere utilizzare soltanto in modo proporzionato e pertinente alle finalità e alla natura delle stesse vigente, di effettuare specifici controlli ad hoc nel caso di segnalazione di attività che abbiano causato danno all'Amministrazione stessa, che ledano diritti di terzi o che siano illegittime.