Centro Servizi per le Imprese
Camera di Commercio Cagliari

Azienda speciale Centro Servizi Promozionali per le Imprese

Regolamento sulla procedura di gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali (data breach) svolti dall'Azienda speciale Centro Servizi Promozionali per le Imprese ai sensi del Regolamento UE 2016/679.

Approvato con deliberazione del Consiglio d'Amministrazione n. 12 del 06/08/2021

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente Procedura è descrivere le attività relative al processo di segnalazione e gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali in qualsiasi modalità svolti dall'Azienda speciale Centro Servizi Promozionali per le Imprese.

Tale processo regolamenta la gestione degli allarmi di sicurezza, la conduzione delle attività funzionali alla individuazione di tutti gli elementi utili alla completa definizione di una violazione, l'attivazione delle strategie di contenimento o delle azioni correttive, la gestione degli adempimenti richiesti dalla normativa nei confronti del Garante per la protezione dei dati personali e degli interessati, le modalità per la tenuta di idonee registrazioni per documentare il rispetto degli obblighi imposti nel rispetto del principio di accountability.

Si precisa che:
a) nei rapporti di contitolarità ciascun Contitolare attua la sua procedura per quanto attiene al trattamento dei dati che svolge. Nell'accordo di contitolarità possono tuttavia essere disposte specifiche procedure e/o modalità relative ad obblighi di comunicazione tra le parti e tra queste ed il garante;
b) per quanto attiene ai data breach relativi alle ipotesi in cui l'Azienda speciale opera in qualità di Responsabile esterno del trattamento, ex art. 28 del Regolamento UE /2016/679, dovranno essere osservate anche le indicazioni e istruzioni fornite dal Titolare nel documento di nomina/designazione.

La presente Procedura è portata a conoscenza, anche attraverso attività di sensibilizzazione o formazione, di tutti i dipendenti dell'Azienda speciale.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Garante per la protezione dei dati personali
WP29	Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) – EDPB (European Data Protection Board)
RPD	Responsabile della protezione dei dati
Delegato del Titolare O Delegato Privacy	Soggetto che, secondo le deleghe/procure formalizzate e il sistema di gestione della privacy, garantisce specifiche funzioni ai fini del rispetto del GDPR – presso l'Azienda speciale unico delegato è il Direttore
Direttore Generale	Direttore dell'Azienda Centro Servizi Promozionali per le Imprese
Evento	Qualsiasi accadimento significativo per la gestione delle infrastrutture IT e per la gestione dell'operatività dei servizi
Violazione (data breach)	Qualsiasi incidente di sicurezza che comporti 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

RIFERIMENTI NORMATIVI

La presente Procedura attua il GDPR con riferimento a:

- art. 33 - *Notifica di una violazione dei dati personali all'autorità di controllo:*
1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

- art. 34 - *Comunicazione di una violazione dei dati personali all'interessato*:
1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

- tenendo conto del documento WP250rev.01, *Guidelines on Personal data breach notification under Regulation 2016/679*, adottato il 3 ottobre 2017 e riemesse il 6 febbraio 2018.

FASI DEL PROCESSO

La gestione di un data breach può riassumersi nelle fasi di seguito elencate:

1. Rilevazione evento;
2. Qualificazione della violazione e rimedi;
3. Invio delle notificazioni;
4. Attività successive.

1. Rilevazione evento.

La rilevazione di un evento può avvenire da diverse fonti:

- SEGNALAZIONE AUTOMATICA: sistemi di segnalazione automatica come quelli che operano per le violazioni derivanti da superamento dei sistemi di Firewall dell'Azienda speciale (gestiti direttamente o tramite soggetti esterni), ovvero gestiti da InfoCamere.

- SEGNALAZIONE INTERNA: a seguito di attività di monitoraggio degli eventi da parte dell'Amministratore di sistema e da parte dei dipendenti, con comunicazione di: malfunzionamenti irrituali o blocco dei sistemi, furti, smarrimenti, intrusioni fisiche nei locali archivio, [anche sulla base di quanto indicato nel Disciplinare sull'uso di internet, posta elettronica ed altri strumenti informatici e telematici], etc.

- SEGNALAZIONE ESTERNA: nell'ambito dell'attività di monitoraggio, assistenza e manutenzione da parte di fornitori esterni di applicativi, supporto sistemistico, servizi di consulenza, etc. ovvero da parte di utenti finali dei servizi dell'Azienda speciale, ovvero da parte di Responsabili esterni nominati ex art. 28 del GDPR.

In particolare, in tutti i contratti che attribuiscano funzioni di Amministrazione di sistemi o deleghino trattamenti di dati personali a soggetti esterni qualificati o qualificabili come Responsabili esterni del trattamento ex art. 28 GDPR, devono essere inserite clausole contrattuali che prevedono l'obbligo:

- di comunicazione immediata di eventuali eventi di sicurezza che abbiano coinvolto i dati oggetto di trattamento, specificando le azioni correttive poste in atto e gli esiti delle stesse. Nello standard contrattuale è previsto che la segnalazione pervenga al responsabile del procedimento;
- di fornire, in caso di necessità, anche attraverso il RPD, la massima disponibilità e collaborazione per l'analisi e risoluzione di eventuali criticità emergenti per l'ambito di trattamento assegnato.

Le segnalazioni pervengono al Delegato Privacy che attiva il primo intervento consistente nella verifica da parte dell'Amministratore di sistema del perimetro dell'evento, ossia di raccogliere e vagliare le seguenti informazioni:

1. sistema, infrastruttura, base dati oggetto dell'evento;
2. tipologia dell'evento verificatosi;
3. tipologia e volume dei dati e degli interessati coinvolti:
4. misure di sicurezza applicate;
5. azioni correttive ipotizzabili.

Il Delegato Privacy individua e avvia le possibili azioni correttive e predispone una Relazione sull'evento che indica le azioni correttive assunte.

Solo nel caso in cui l'evento coinvolga dati personali, il Delegato attiva il secondo intervento in cui si sostanzia la seconda fase della procedura.

La fase di rilevazione evento deve concludersi entro 24 ore dalla conoscenza dello stesso evento.

Al riguardo, si precisa che il momento esatto in cui il Titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

2. Qualificazione della violazione e rimedi

Qualora l'incidente coinvolga dati personali il Delegato Privacy trasmette la Relazione sull'evento di cui alla precedente fase al Responsabile della Protezione dei Dati e costituisce un apposito gruppo di lavoro costituito da:

- il RPD dell'Azienda speciale;
- il responsabile del processo in relazione al quale si ipotizza la violazione di dati;
- l'Amministratore di sistema;
- lo specialista della società o soggetto che ha realizzato o fornito il prodotto o servizio interessato dall'incidente e/o il RPD (ove nominato) o altro referente specializzato della Società coinvolta nel trattamento;
- l'eventuale consulente tecnico o giuridico qualora necessario.

Il gruppo di lavoro ha il compito di verificare, a norma dell'art. 33, par. 1, del GDPR, la probabilità che la violazione dei dati personali presenti un rischio (soprattutto se questo può qualificarsi come "elevato") per i diritti e le libertà delle persone fisiche e, di conseguenza, decidere le misure di risposta all'emergenza.

A tal fine:

a) sono raccolte e approfondite le informazioni necessarie, ove disponibili, per l'eventuale compilazione del Modello per la notificazione al Garante, rinvenibile nel sito dell'Autorità;

b) sono effettuate le seguenti valutazioni:
- natura della violazione e potenziale esposizione degli interessati (c.d. gravità dell'accadimento);
- priorità, in funzione dell'urgenza (valutata sulla base di quanto velocemente potrebbero verificarsi danni);
- impatto potenziale dell'esposizione degli interessati (valutazione dell'entità dei danni agli interessati)[1];
- adeguatezza delle misure di sicurezza già implementate rispetto al potenziale danno arrecabile agli interessati.

Per un quadro delle valutazioni dei rischi si rinvia anche a quanto contenuto nelle Linee guida del WP29 (WP250rev.01).

All'esito dell'analisi:

A. nel caso in cui la violazione – in funzione dell'adeguatezza delle misure implementate – non costituisca un rischio per gli interessati, il Delegato Privacy provvede a verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD; copia del verbale deve essere inviato al RPD che provvede ad aggiornare il "Registro dei Data Breach" come da format allegato (All. 2);

B. nel caso in cui sia stato valutato che le misure implementate siano insufficienti alla tutela degli interessati:

1. il gruppo di lavoro provvede a identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata e il miglior esito ai fini della minimizzazione del possibile danno agli interessati;
2. il Delegato provvede a:

- definire e assegnare responsabilità e tempistiche per rimediare all'incidente, compresi i soggetti esterni coinvolti;
- verbalizzare gli esiti dell'analisi riportando esplicitamente il parere formalizzato dal RPD;
- decidere se procedere o meno alle notificazioni;
- compilare eventualmente il Modello per la notificazione al Garante, nella sua versione vigente, così come pubblicato nel sito internet dell'Autorità e secondo le relative istruzioni operative, indicando se le azioni correttive sono già concluse o ancora *in itinere*;
- predisporre, qualora ne ricorrano le condizioni, la comunicazione da inviare all'interessato (ovvero la comunicazione pubblica), contenenti le indicazioni riportate nell'All. 1.

La seconda fase deve concludersi entro ulteriori 36 ore dalla conoscenza dell'evento.

[1] Ovvero danno fisico, materiale o immateriale, in particolare: perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti; discriminazioni; furto o usurpazione d'identità; perdite finanziarie; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale; decifratura non autorizzata della pseudonimizzazione; qualsiasi altro danno economico o sociale significativo" (considerando 75 e 85 GDPR).

3. Invio delle notificazioni.

Il Modello deve essere sottoscritto con firma digitale dal Direttore e inviato formalmente al Garante nel più breve tempo possibile, **possibilmente entro 72 ore** dall'avvenuta conoscenza da parte del Titolare, di un evento qualificabile come Data breach.

Ove avvenga oltre tale limite temporale è necessario corredarla dei motivi del ritardo[2].

Qualora non si disponga di tutte le informazioni previste dal Modello, è possibile inviare una prima notifica parziale, da completare non appena disponibili le ulteriori informazioni.

Il Direttore invia il verbale di cui alla fase precedente (lettera B) e il Modello da lui stesso sottoscritto:

- al RPD che aggiorna o provvede a far aggiornare il "Registro dei Data Breach";
- al referente dell'Amministrazione Pubblica da cui eventualmente l'Azienda ha ricevuto l'incarico di trattare i dati personali[3], previa valutazione di opportunità condotta congiuntamente con il Direttore e a seguito dell'avvenuta notifica al Garante.

Ove le misure di cui al punto B) del paragrafo precedente siano adottate immediatamente, la fase si chiude con una verbalizzazione, da parte del Direttore, degli adempimenti seguiti, con la precisazione che, a norma dell'art. 34, par. 3, lett. b, del GDPR, non è richiesta la comunicazione all'interessato se il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i suoi diritti e libertà.

Nel caso in cui tali misure necessitino di maggior tempo per l'implementazione ovvero non siano in grado di minimizzare i rischi per gli interessati, il Direttore:

a) provvede a definire i contenuti della comunicazione agli interessati, che – con linguaggio semplice e chiaro – deve contenere almeno i seguenti elementi:
   - la natura della violazione dei dati personali;
   - le probabili conseguenze della violazione dei dati personali;
   - le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione;
   - il nome e i dati di contatto del Responsabile della protezione dei dati;

   la comunicazione – un cui esempio è riportato nell'All. 1 – è sottoposta a parere del RPD e ad approvazione del Direttore.

b) verifica la fattibilità di reperimento dei dati di contatto degli interessati coinvolti o potenzialmente coinvolti; nel caso in cui si valuti che la comunicazione agli interessati possa essere sostenuta senza sforzi sproporzionati (ad es., disponibilità di email/pec), provvede all'invio massivo della comunicazione.

c) ove non vi sia disponibilità di dati di contatto ovvero si valuti che la comunicazione richieda sforzi sproporzionati, provvede a darne pubblicità nelle modalità concordate con il Direttore e il RPD (ad es., pubblicazione in evidenza sul sito istituzionale, comunicati stampa, etc.).

La comunicazione agli interessati deve essere formalizzata "senza ingiustificato ritardo".

Dell'avvenuta comunicazione è data informazione al RPD.

Si precisa che:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche.

---

[2] ad es., data breach particolarmente complesso, serie di attacchi/violazioni consecutive che necessitano di una reazione complessa.

[3] ad es., sulla base di una convenzione/protocollo d'intesa.

4. Attività successive.

Se durante le fasi precedenti si sospetta che la violazione possa essere stata provocata in maniera intenzionale da un esterno o da un utente interno si attiva il processo di raccolta delle evidenze o prove con investigazioni anche difensive.

L'attività, ove necessario, può essere gestita secondo quanto previsto dall'art. 391 nonies[4] o dall'art. 327 bis c.p.p.[5] e deve rispettare gli standard e le normative (raccolta e "catena di custodia") in termini di analisi forense, al fine di poter intraprendere successivamente un'azione legale nei confronti dell'eventuale responsabile.

Qualora non si riscontrasse questa condizione, l'analisi post-violazione sarà finalizzata all'apprendimento delle cause che hanno generato l'evento al fine di imparare dai propri errori e per fornire ulteriori informazioni per la risoluzione di eventuali criticità collegate o ricorrenti.

All'esito delle notificazioni al Garante e agli interessati, il RPD deve:

- gestire in prima persona le relazioni e gli eventuali feedback pervenuti dal Garante e dalle altre Istituzioni coinvolte, coordinando – con l'ausilio della sua struttura di supporto – l'aggiornamento del "Registro dei Data Breach" (un cui modello è riportato nell'All. 2);
- gestire le comunicazioni, istanze e richieste da parte degli Interessati, anche attraverso un referente della Segreteria di Direzione, ovvero del Settore di riferimento interessato dalla la violazione.

FORMAZIONE

Nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, l'Ente svolge attività di informazione e formazione con riferimento ai contenuti del presente documento.

4 Se precedente all'instaurazione di un procedimento penale.

5 Se già instaurato il procedimento.

ALLEGATO 1 – MODELLO DI COMUNICAZIONE ALL'INTERESSATO (6*)

Denominazione del Titolare del trattamento	
Dati di contatto	
Soggetto che effettua la notifica	
Ruolo del soggetto che effettua la notifica	
Responsabile della Protezione dei dati	
Dati di contatto del RPD	

Interessato destinatario della comunicazione	

Modalità della comunicazione

- ☐ Raccomandata A/R
- ☐ PEC
- ☐ Posta elettronica
- ☐ Fax
- ☐ Altro: _____

Spett. Società/Egr. Sig……./

siamo spiacenti di informare che in data …….. abbiamo rilevato di aver subito una violazione dei dati personali La riguardano.

Nel prosieguo, in termini sintetici, è fornito – ai sensi di quanto previsto dall'art. 34 Regolamento UE 2016/679 (GDPR) – un quadro di quanto è accaduto.

La violazione è stata anche notificata al Garante.

Breve descrizione della violazione di dati personali e delle sue modalità

6 (*) Qualora la comunicazione richieda – ex art. 34, par. 3, lett. c) del GDPR – uno sforzo sproporzionato (in relazione, per es. alle attività da svolgere e/o ai costi da sostenere), "(…) si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia".

Dispositivo oggetto della violazione

☐ Computer
☐ Dispositivo mobile
☐ Documento cartaceo
☐ File o parte di un file
☐ Strumento di back-up
☐ Rete
☐ Altro:

Tipologia di dati coinvolti nella violazione

☐ Dati anagrafici
☐ Numero di telefono (fisso o mobile)
☐ Indirizzo di posta elettronica
☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
☐ Altri dati di personali (sesso, data di nascita, età, ...), dati particolari, sanitari e giudiziari
☐ Ancora sconosciuto
☐ Altro:

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
☐ Altro:

Livello di gravità della violazione dei dati personali e possibili conseguenze

Indicare:

A) Numero approssimativo di registrazioni dei dati personali oggetto della violazione
B) Categoria e numero approssimativo degli interessati coinvolti dalla violazione
C) Livello di gravità elevato della violazione per i diritti e le libertà delle persone fisiche
D) Possibili conseguenze della violazione.

(secondo le valutazioni del Titolare)

Misure tecniche e organizzative applicate preventivamente e quelle applicate successivamente alla violazione per porre rimedio alla violazione o per attenuarne le conseguenze

Per ulteriori informazioni, può essere contattato ……

ALLEGATO 3 – REGISTRO DEI DATA BREACH

N./anno	Banca dati/Archivio coinvolto dalla violazione	Processo/progetto e Ufficio di riferimento	Cause della violazione (vulnerabilità)	Tipologia e modalità di realizzazione	Conseguenze della violazione	Azioni correttive adottate	Esiti delle azioni correttive	Notifica al Garante (sì/no) [indicare protocollo comunicazione]	Notifica agli Interessati (sì/no) [indicare protocollo comunicazione]	Prescrizioni specifiche del Garante