LORAN

LORAN S.r.l. Via Delle Ginestre 14/16/18 - 70026 MODUGNO (BA)

+39 080 5427032 pbx
+39 080 5426903
info@loransrl.net | loran@pec.it
loransrl.net

ANALISI DEI RISCHI

Sommario

1. INTRODUZIONE

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

In caso di violazione dei dati personali, Il Regolamento Ue 2016/679 dispone che il titolare del trattamento notifichi la violazione all'Autorità Garante per la protezione dei dati personali (Autorità) 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, la stessa è corredata dei motivi del ritardo (art 33, par 1). Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta al titolare.

In caso di rischi elevati per i diritti e le libertà, si dovranno informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo" fatte salve alcune eccezioni (art. 34 paragrafo 3 Regolamento UE 2016/679). In ogni caso, tutti i titolari del trattamento dovranno documentare le violazioni dei dati personali subiti, anche se non notificate all'autorità di controllo e non comunicate agli interessati.

Il titolare dovrà documentare accuratamente le circostanze, le conseguenze e le contromisure adottate al fine di impedire che un evento simile si verifichi in futuro. Il titolare è tenuto ad esibire la documentazione, su richiesta, all'Autorità Garante, in caso di accertamenti (Art. 33 paragrafo 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*".

2. SCOPO E CAMPO D'APPLICAZIONE

La presente procedura disciplina la modalità di gestione delle violazioni di dati personali, ivi inclusi gli obblighi di notifica all'Autorità ed agli interessati ove applicabile e le modalità per documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati.

La presente procedura si applica a tutti i dipendenti della società LORAN, senza distinzione di ruolo e livello e a tutti i collaboratori che a qualunque titolo svolgono la loro attività per conto della società (es. tirocinanti, stagisti, studenti universitari, consulenti, collaboratori a progetto).

Il presente documento si applica anche ai dipendenti di società esterne affidatarie di servizi da parte di LORAN, nominati Responsabili del trattamento.

3. DEFINIZIONI

Violazione di dati personali - Per violazione dei dati personali (data breach) si intende la divulgazione (intenzionale o non), la distruzione, la perdita, la modifica o l'accesso non autorizzato ai dati trattati da aziende o pubbliche amministrazioni. La violazione dei dati personali, quindi, non è rappresentata solo da un attacco informatico, ma può essere anche un accesso abusivo, un incidente (es. un incendio o una calamità naturale), la semplice perdita di una chiavetta USB o la sottrazione di documenti con dati personali, il furto di un notebook di un dipendente. In sostanza la violazione dei dati personali racchiude un ventaglio molto ampio di eventi avversi che comprometterebbero i dati personali e di conseguenza la dignità e le libertà fondamentali dell'individuo a cui si riferiscono.

Incidente e violazione - È necessario esplicitare la differenza terminologica tra incidente e violazione dei dati personali. Con l'incidente non si verifica il furto e la divulgazione di dati personali che invece si verifica con la violazione che comprometterebbe la confidenzialità, l'integrità e la disponibilità del dato.

Grado di rischio – tipologia e livello di danno, fisico, materiale o immateriale che una violazione può comportare alle persone fisiche quali ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, quali ad esempio: "discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali

protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata". In assenza di ulteriori indicazioni, il considerando n. 85 del Regolamento offre alcuni criteri per delimitare il "rischio" che una violazione dei dati personali può comportare.

4. TIPOLOGIA DI VIOLAZIONI E CAUSE

Di seguito sono esplicitate a titolo indicativo e non esaustivo le tipologie di violazioni e le possibili cause.

4.1. Tipologia di violazioni

4.1.1 Fisica

- Accesso abusivo in ambienti di lavoro riservati
- Lettura, copia e fotografia di documenti contenenti dati personali;
- Sottrazione di documenti cartacei
- Sottrazione di computer, supporti di memorizzazione e di altri dispositivi elettronici contenenti dati personali

4.1.2 Logica

- Accesso abusivo alla postazione di lavoro (PdL)
- Furto di credenziali di accesso
- Indisponibilità dei dati e delle informazioni del data center aziendale
- Alterazione dei dati (crittografia da virus)
- Perdita di confidenzialità/riservatezza dei dati
- Perdita di memorie USB non cifrate sulle quali sono stati copiati dati personali e particolari di dipendenti;
- Supporti di memorizzazioni distrutti e/o rovinati, sottratti

4.2. Possibili cause di violazioni

4.2.1 Utilizzo scorretto della Postazione di lavoro, dei dispositivi mobili (notebook, tablet e smatphone) e dei supporti di memorizzazione (chiavette USB, CD)

- Postazione di lavoro incustodita e non bloccata (assenza del salvaschemo)
- Memorizzazione delle credenziali nei software
- Annotazione delle credenziali in prossimità della postazione di lavoro
- Scelta di password deboli (quali ad esempio nome, cognome, data di nascita, 12345678)
- Uso di un algoritmo noto per la creazione di password per gli utenti
- Lasciare incustoditi o perdere supporti di memorizzazione USB non protetti da password e non cifrati e contenenti dati personali e particolari

4.3. Eventi con effetti sul data center aziendale

- Guasto fisico al sistema servente
- Anomalie software dei Sistemi Operativi
- Anomalie nei sistemi di alimentazione elettrica
- Anomalie nei sistemi di raffrescamento
- Eventi naturali, (inondazioni, terremoti, ecc.)
- Azioni derivanti da maleware
- Azioni di Denial of Service
- Intercettazioni di rete (Man in The Middle)
- Utilizzo delle credenziali di default nei database
- Escalation dei privilegi derivante da maleware
- Errore di configurazione degli account utente e delle relative autorizzazioni
- Utilizzo di credenziali amministrative, con maggiori privilegi, da parte degli utenti

5. RESPONSABILITÀ

5.1. Tutto il personale

Tutti coloro che trattano i dati personali per conto di LORAN, che vengono a conoscenza di una potenziale o violazione certa sui sopracitati dati, sono obbligati a segnalare tempestivamente l'accaduto al Responsabile del Reparto presso la quale si presta la propria opera.

5.2. Responsabili di Reparto

Secondo il modello organizzativo adottato, i Responsabili di Reparto devono segnalare tempestivamente al Titolare del trattamento e al Responsabile della Protezione Dati (RPD) l'evento avverso verificatosi nel reparto di responsabilità e collaborare alla corretta gestione dell'iter per la violazione.

5.3. Responsabili del trattamento (fornitori e manutentori)

I Responsabili del trattamento nominati ai sensi dell'Art. 28, devono, senza ingiustificato ritardo, segnalare tempestivamente al Titolare del trattamento e al Responsabile della Protezione Dati (RPD) l'evento avverso verificatosi sui sistemi, sui trattamenti e/o sui dati personali e particolari, che in virtù del rapporto contrattuale, possono venire a conoscenza. In caso di una violazione sospetta o certa il Responsabile deve collaborare per la corretta gestione dell'incidente.

5.4. Contitolari

L'articolo 26 riguarda i contitolari del trattamento e specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del regolamento. Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. Il Gruppo di lavoro WP29 raccomanda che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento. In presenza di una violazione sospetta o certa il primo dei Contitolare che viene a conoscenza dell'evento avverso deve, senza ingiustificato ritardo, segnalare

tempestivamente all'altro Titolare del trattamento e al Responsabile della Protezione Dati (RPD) di competenza l'evento avverso verificatosi che ha visto coinvolti di dati personali e/o particolari. In virtù di quanto disciplinato nel rapporto contrattuale, sarà responsabile della corretta gestione dell'incidente. Entrambi dovranno collaborare per la corretta gestione della violazione.

5.5. Titolare

Il titolare del trattamento non appena riceve una segnalazione di una potenziale o violazione certa dei dati personali ha la responsabilità di avviare e gestire l'iter per la violazione ponendo in essere:

- l'attività conoscitiva
- la valutazione del rischio e delle conseguenze per gli interessati
- la notifica della violazione all'Autorità ed agli interessati, ove applicabile, senza ingiustificato ritardo e ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza.
- il ripristino e la mitigazione del rischio.

Inoltre, il titolare ha la responsabilità di documentare le violazioni dei dati personali subite, anche se non notificate all'Autorità di controllo e non comunicate agli interessati.

5.6. Responsabile Protezione Dati

Il Responsabile della Protezione dati fornisce consulenza al titolare coadiuvandolo nella gestione dell'iter per la valutazione della violazione, sorvegliando l'osservanza del regolamento e fungendo da punto di contatto per l'Autorità (art.39 par1).

6. MODALITÀ PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

Il Regolamento Europeo per la Protezione dei Dati Personali individua perentoriamente il termine massimo di 72 ore entro il quale deve essere comunicato all'Autorità di controllo l'evento avverso verificatosi sui dati personali e le potenziali conseguenze della violazione sui diritti e le libertà fondamentali degli individui a cui si riferiscono i dati.

Di seguito vengono descritte le attività che dovranno essere espletate non appena si viene a conoscenza di un evento avverso/violazione dei dati personali raggruppate in quattro fasi.

Figura 1: Rappresentazione schematica dell'iter per la gestione della violazione

6.1. Fase 1 Segnalazione al Titolare e al RPD

Tutti coloro che vengono a conoscenza di una violazione certa o presunta dei dati personali dovranno tempestivamente segnarlo al Responsabile del reparto presso la quale prestano la propria opera.

Il Responsabile del reparto tramite l'allegato 1, dovrà tempestivamente segnalare l'accaduto al Titolare e al RPD attraverso il modello di comunicazione della violazione dei dati personali, allegata alla presente procedura segnalando, obbligatoriamente, le seguenti informazioni necessarie ad avviare l'istruttoria:

- Denominazione della/e banca/banche dati oggetto di violazione e una breve descrizione di quanto accaduto e dei dati personali coinvolti
- Data e ora dell'evento
  - Un eventuale intervallo di tempo nel quale si è verificato l'evento (se noto)
  - Se l'evento è ancora in corso
  - Oppure se non si riesce a determinare l'esatta insorgenza dell'evento avverso

- Descrizione del luogo in cui si è verificato l'evento specificando se è avvenuto in seguito ad uno smarrimento di un dispositivo elettronico, una memoria USB, o semplicemente lo smarrimento o sottrazione di un documento cartaceo
- Indicazione del tipo di esposizione al rischio e se si sia verificata il seguente tipo di violazione:
  - Lettura (presumibilmente i dati non sono stati copiati)
  - Copia (i Titolare è ancora in possesso dei dati)
  - Alterazione (i dati sono presenti ma sono stati alterati)
  - Cancellazione/distruzione (i dati non sono più posseduti dal titolare e non li ha neppure l'autore della violazione)
  - Furto (i dati non sono più posseduti dal titolare, sono ora in possesso dell'autore della violazione)
- Indicazione del dispositivo oggetto della violazione:
  - Computer
  - Rete
  - Dispositivo mobile
  - File o parte di un file
  - Strumento di backup
  - Documento cartaceo

6.2. Fase 2 rilevazione/accertamento della violazione (attività conoscitiva)

Il Titolare, supportato dal RPD, individua un team per la gestione dell'incidente, nel quale ogni soggetto coinvolto ha delle specifiche responsabilità.

L'assegnazione dei ruoli deve quindi essere sufficientemente precisa da consentire l'identificazione univoca di specifici gruppi di persone che eseguono ciascuna azione (nella maggior parte dei casi un soggetto responsabile e un sostituto devono essere identificati).

Pertanto, il team "incident response" che deve gestire l'istruttoria, deve essere composto in funzione della tipologia della violazione, come di seguito indicato.

6.2.1. Eventi riguardanti una violazione fisica: figure coinvolte

Se l'evento riguarda una violazione fisica che ha compromesso le informazioni personali contenute nei documenti cartacei faranno parte del team incident response: il Titolare coadiuvato dall'RPD e il Responsabile del reparto in cui si è verificato l'evento. L'istruttoria sarà focalizzata sulle misure di sicurezza fisiche e sulle misure organizzative adottate nel reparto e sulle eventuali azioni di mitigazione già in corso, evidenziandole in un arco temporale.

6.2.2. Eventi riguardanti una violazione informatica: figure coinvolte

Nel caso di eventi avversi riguardanti i dati e i documenti informatici, faranno parte del team incident response: il Titolare coadiuvato dall'RPD, il Responsabile dell'Ufficio Informatico, l'Amministratore di Sistema dell'infrastruttura violata ed il Responsabile del reparto in cui si è verificato l'evento. Se la violazione è avvenuta sui dispositivi informatici presenti nel reparto, l'istruttoria sarà focalizzata sulle misure di sicurezza informatiche e sulle misure organizzative adottate nel reparto. Nell'eventualità che la violazione sia stata perpetrata nei confronti dell'infrastruttura informatica aziendale le attività forensi per l'individuazione delle cause e conseguenze saranno svolte a cura del Responsabile dell'Ufficio Informatico e dell'Amministratore di sistema di competenza. Saranno, inoltre, prese in considerazione le eventuali azioni di mitigazione già in corso, evidenziandole in un arco temporale.

6.2.3. Eventi riguardanti la videosorveglianza: figure coinvolte

Nel caso di eventi avversi riguardanti la videosorveglianza, faranno parte del team incident response: il Responsabile della videosorveglianza, il manutentore/amministratore dei sistemi di videosorveglianza, con la collaborazione del RPD e con il Responsabile del

Reparto in cui si è verificato l'evento. L'attenzione sarà posta sulle misure di sicurezza tecniche ed organizzative adottate.

6.3. Fase 3 Analisi della violazione, valutazione dei rischi connessi e notifica

In questa fase ogni componente del team incident response, per quanto di competenza, deve acquisire e valutare le evidenze al fine di individuare il livello di gravità della violazione nei confronti dei dati personali e determinare le conseguenze per i diritti e le libertà degli interessati.

Al fine di calcolare il livello dell'impatto e la gravità delle conseguenze derivanti da una violazione dei dati personali, si è ritenuto opportuno fare riferimento alle raccomandazioni elaborate dall'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA) (vedi Allegato 2: Recommendations for a methodology of the assessment of severity of personal data breaches).

6.3.1. Violazione di dati: assenza di rischio

Nel caso in cui la violazione dei dati personali non determini alcuna compromissione ai diritti e alla libertà fondamentali dell'individuo, non è obbligatoria la notifica all'Autorità ma è comunque necessario comprovare l'assenza dei rischi. Inoltre, è necessario registrare la violazione in un apposito registro.

6.3.2. Violazione di dati: presenza di rischi

In presenza di rischi per gli interessati il Titolare per il tramite del RPD, notifica la violazione all'Autorità di controllo entro 72 ore all'Autorità Garante Privacy, utilizzando l'apposita modulistica (all. 2 modello di comunicazione all'Autorità Garante per la Protezione dei Dati Personali). Qualora la notifica non sia effettuata entro 72 ore, la stessa è corredata dai motivi del ritardo.

6.3.3. Notifica della violazione all'Autorità di Controllo

A cura del RPD, entro 72 ore, devono essere effettuate le seguenti attività:

a) Organizzazione delle informazioni raccolte e predisposizione della notifica della violazione dei dati personali all'Autorità che deve contenere:
   - una descrizione sintetica dei sistemi di elaborazione, di memorizzazione dei dati se la violazione riguarda un dato informatico o la descrizione della modalità di gestione dei documenti cartacei. Per entrambi i casi indicare l'esatta ubicazione delle informazioni personali oggetto di violazione
   - il numero dei soggetti coinvolti nella violazione che possono essere determinati o stimati
     - n. _____ persone
     - circa _____persone
     - un numero (ancora) sconosciuto di persone
   - le tipologie di dati oggetto di violazione
     - dati anagrafici/codice fiscale
     - dati di accesso e di identificazione (username, password, customer ID, altro)
     - dati relativi a minori
     - dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
     - dati personali idonei a rivelare lo stato di salute e la vita sessuale
     - dati giudiziari
     - copia per immagine su supporto informatico di documenti analogici
     - ancora sconosciuto
     - Altro
   - le misure tecniche ed organizzative che sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future
   - l'indicazione dell'avvenuta comunicazione agli interessati, ove applicabile, e con quale mezzo
     - Sì, è stata comunicata il _____
     - No, perché _____
   - il testo della comunicazione resa agli interessati

b) Invio della notifica all'Autorità

c) Registrazione degli eventi

Qualunque sia l'esito dell'evento, questo deve essere annotato in un registro immodificabile ed a disposizione dell'autorità di controllo.

d) Conservazione del registro delle violazioni

6.4. Fase 4 – avvio delle azioni correttive

I componenti del team incident response impegnati nella gestione della violazione devono individuare tempestivamente:

- le strategie per ripristinare il servizio o i dati personali compromessi
- mitigare il rischio ed individuare le misure correttive in tal senso.

7. ARCHIVIAZIONE DEI DOCUMENTI

La documentazione relativa alla gestione delle violazioni dei dati personali su supporto cartaceo viene conservata in doppia copia presso la Direzione Amministrativa e l'ufficio protezione dei dati personali.

La documentazione relativa alla gestione delle violazioni dei dati personali riguardanti i dati ed i documenti informatici viene conservata in doppia copia presso l'ufficio Informatico e l'ufficio protezione dei dati personali.

Il Registro delle violazioni, se non ancora informatizzato, deve essere custodito da parte dell'Ufficio protezione dati personali ed a disposizione dell'Autorità di controllo.

8. STORIA DELLE MODIFICHE

Revisione	Data Emissione	Esito
00	Agosto 2018	Prima stesura
01	Novembre 2018	Prima emissione

9. ALLEGATI

Allegato 1: Modello di comunicazione al Titolare/RPD

Allegato 2: Violazione di dati personali - modello di comunicazione al garante

Allegato 3: Recommendations for a methodology of the assessment of severity of personal data breaches.