



LA NOSTRA POLITICA DELLA PRIVACY

Edizione Gennaio 2021

Sommario

<u>La Tutela Dei Dati E Della Privacy In 3EGECO Investimenti</u>	2
<u>Ruoli Nelle Politiche Della Privacy</u>	3
<u>Vademecum Sui Dati Personali</u>	4
<u>Vademecum Sugli Amministratori Di Sistema</u>	4
<u>Finalità E Modalità Del Trattamento</u>	5
<u>Rapporti Con La Clientela</u>	6
<u>Metodologie Di Progettazione Ed Implementazione</u>	8
<u>Gestione Dei Data Breach</u>	9
<u>Trasferimento Dei Dati</u>	11
<u>Formazione</u>	11
<u>Contatti</u>	12



LA TUTELA DEI DATI E DELLA PRIVACY IN 3EGECO

Finalità

3EGECO S.r.l. è una società partecipata da Elettra Investimenti S.p.A., holding industriale i cui titoli sono negoziati sul mercato AIM – Italia che opera sul territorio nazionale per la realizzazione e lo sviluppo di progetti nel settore energetico che si occupa, tra l'altro, anche di strutturare e gestire il processo finalizzato alla riqualificazione energetica del patrimonio immobiliare permettendo ai proprietari di beneficiare degli incentivi previsti dal D.L. n. 34/20 (c.d. “Decreto Rilancio”), convertito nella L. n. 77/20.

Ha sede legale in Via Borgonuovo, 27 – 27121 Milano e sede operativa in Via Duca del Mare, 19 - 04100 Latina (LT), di seguito viene per brevità denominata “3EGECO” ed ha una propria politica della privacy e della tutela dei dati coerente con i dettami normativi del Regolamento Europeo sulla privacy n°679/2016 e successive integrazioni.

Scopo del presente documento è certificare le modalità con le quali 3EGECO opera in conformità ai sensi dell'Articolo 40 del suddetto regolamento, certificando procedure, misure tecniche ed organizzative adeguate ai servizi erogati alla propria Clientela.

Accountability

3EGECO assicura la massima tutela dei dati dei propri trattamenti garantendo la tutela dei trattamenti effettuati per mezzo di Responsabili esterni.

L'obiettivo è di operare e cooperare in linea con il principio di “accountability” citato nell'articolo 5 del regolamento Europeo 679/2016, trattando dati personali e particolari con la consapevolezza che si tratta di informazioni di Terzi e che responsabilmente si deve individuare ogni azione possibile per prevenire qualsiasi uso improprio delle informazioni stesse.

Operatività

3EGECO eroga i propri servizi in qualità di Titolare del trattamento, per gli ambiti di dati personali e particolari afferenti ai propri Clienti ed ai propri Collaboratori, ed opera quale Responsabile Esterno del trattamento, per gli ambiti di trattamento con il quale interagisce in relazione ai contratti di servizi con i propri Clienti.

3EGECO è attenta alla soddisfazione di alcuni principi basilari:

- implementare le proprie procedure, i sistemi e l'operatività in una logica che soddisfi i principi della “privacy by design” e della “privacy by default”, sin dalle fasi di progettazione come previsto dall'articolo 25 del Regolamento Europeo 679/2016;
- assicurare che la propria Clientela abbia piena consapevolezza delle tutele poste in atto da 3EGECO, opportunamente differenziate per ciascuna tipologia di servizio erogato;
- tutelare le informazioni personali contenute nei propri trattamenti assicurando il pieno rispetto di quanto previsto dall'articolo 5 del Regolamento Europeo 679/2016, ovvero:



- o liceità, correttezza e trasparenza, raccogliendo informazioni per finalità determinate e condivise;
- o legittimità, limitando gli accessi a quanto necessario rispetto alle finalità per le quali sono trattati, verificandone esattezza, coerenza ed adottando tutte le misure ragionevoli per eliminazioni e/o modifiche;
- o conservazione, in forme che consentano l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- o protezione, adottando misure tecniche e organizzative adeguate impedendo trattamenti non autorizzati o illeciti, protetti dalla perdita, dalla distruzione o dal danno accidentali;

3EGECO opera secondo i dettami delle politiche di qualità, protesa al miglioramento continuo ed alla ricerca delle soluzioni e delle procedure maggiormente efficaci in una logica di contenimento dei rischi correlati ai trattamenti.

RUOLI NELLE POLITICHE DELLA PRIVACY

Titolare del Trattamento

L'articolo 4 del Regolamento Europeo 679/2016 stabilisce che il Titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

3EGECO è titolare del trattamento per i dati personali e particolari gestiti nell'ambito del proprio business, come ad esempio dati personali di propri Clienti e Collaboratori.

Responsabile della Protezione dei Dati

3EGECO, in conformità all'articolo 37 del Regolamento Europeo 679/2016, ha costituito un ufficio privacy ed ha nominato un proprio responsabile della protezione dei dati che può essere contattato sull'indirizzo e-mail privacy@3egeco.it

3EGECO si riserva di poter contattare il Responsabile Protezione Dati del Cliente o del Responsabile esterno, ove presente, in ogni occasione correlata ad azioni che abbiamo impatto su trattamenti di dati personali e particolari, al fine di garantire continuativamente che i propri servizi soddisfino i principi della tutela della privacy by design e della tutela della privacy by default.

Responsabile Esterno del Trattamento

L'esecuzione dei trattamenti di dati personali su commissione, come ad esempio il trattamento di buste paga o prescrizioni sanitarie, prevede la nomina di un responsabile esterno del trattamento.

La nomina ha efficacia laddove disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincola il Responsabile esterno del trattamento al Titolare del trattamento.



Nell'atto sono descritti materia disciplinata e durata del trattamento, natura e finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

I Responsabili esterni del trattamento sono nominati da 3EGECO previo accertamento di adeguate garanzie sulle misure tecniche ed organizzative adottate a fronte di certificate competenze.

Per ogni trattamento, 3EGECO assicura che:

- i dati personali sono trattati su istruzione documentata agli Incaricati preposti;
- gli Incaricati al trattamento garantiscono assoluta riservatezza nell'espletamento delle proprie mansioni e sono adeguatamente e periodicamente formati;
- sono adottate tutte le misure richieste ai sensi degli articoli 32, 33, 34, 35 e 36 del GDPR;
- non si ricorre a Contitolari del trattamento;
- vengono eliminati o restituiti dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento ed è terminato il periodo di conservazione obbligatoria dei dati;

Nello svolgimento del proprio ruolo di Titolare del trattamento, 3EGECO è coadiuvata da proprie risorse caratterizzate dal profilo di incaricato al trattamento. Dietro apposita autorizzazione, definita lettera di incarico, effettuano materialmente operazioni di trattamento sui dati personali attenendosi alle istruzioni impartite.

Per tale fine ricevono una specifica autorizzazione, corredata da istruzioni, in merito alle responsabilità ed ai compiti afferenti alla sfera dei dati personali con i quali entra in contatto durante l'espletamento della propria mansione.

Gli incaricati sono oggetto di audit periodici relativamente alle performance ed alla compliance.

VADEMECUM SUI DATI PERSONALI

Per "dati personali" si intendono informazioni di natura personale o particolare, in formato cartaceo o digitale, a cui 3EGECO accede nell'ambito dell'esecuzione dei contratti di servizi o di lavoro sottoscritti con Persone fisiche.

I dati:

- Sono afferenti ad "interessati" per i quali il Titolare del Trattamento ha acquisito regolare consenso al trattamento conforme ai dettami normativi.
- Sono conservati e/o eliminati e/o restituiti secondo indicazioni specifiche ricevute dal Cliente.
- Non sono accessibili per finalità difformi dall'oggetto del contratto di erogazione dei servizi.
- Non sono accessibili da Incaricati che non abbiano specifica autorizzazione al trattamento.
- Non sono oggetto di diffusione o cessione a terzi.
- Ove possibile vengono anonimizzati.
- Sono trasmessi a Responsabili esterni esclusivamente in modalità protetta e crittografata.



3EGECO ha progettato ed implementato adeguati sistemi di accesso e protezione dei suddetti dati, sia a livello fisico e perimetrale, sia a livello logico per i dati conservati e gestiti su sistemi informatici.

3EGECO non tratta dati personali e/o particolari per il quali in via diretta o attraverso il proprio Cliente non abbia evidenza del consenso al trattamento.

VADEMECUM SUGLI AMMINISTRATORI DI SISTEMA

Con la definizione di amministratore di sistema si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

3EGECO, in ottemperanza alla normativa, considera amministratori di sistema anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, amministratori di reti e di apparati di sicurezza e amministratori di sistemi software complessi (che ad esempio detengono diritti di profilazione di utenti in termini di accesso a dati personali e particolari).

L'operato degli amministratori di sistema è oggetto di verifica annuale da parte da parte del Titolare del trattamento, al fine di verificare rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti. Si prospettano due scenari, che contemplano uno o più soggetti interni o esterni all'organizzazione:

Il ruolo di Amministratore di sistema esterno è contemplato nell'atto con il quale sono evidenziate le specifiche funzioni attribuite e sono elencate in maniera analitica tutte le attività che verranno svolte.

Gli accessi ai sistemi da parte degli Amministratori di sistema di 3EGECO sono oggetto di registrazione su un file di log, unitamente ad ogni informazione che è possibile tracciare in merito alle attività svolte. Il file è crittografato e contiene i log di un periodo non inferiore agli ultimi sei mesi.

FINALITÀ E MODALITÀ DEL TRATTAMENTO

Finalità del Trattamento

I dati al quale 3EGECO può avere accesso, attraverso propri Collaboratori espressamente incaricati e formati, sono afferenti alle gestioni del proprio business e sono correlati all'esecuzione del contratto di erogazione di servizi in essere con il Cliente.

I dati vengono trattati in conformità alle prescrizioni in materia di liceità del trattamento previste dal Regolamento Europeo 679/2016.

Le tipologie di dati trattati possono essere raggruppate nell'elenco seguente:

- Dati amministrativi per finalità fiscali e contabili, tra le quali documenti di vendita cartacei ed elettronici, dichiarazioni di redditi, documenti di trasporto, libri contabili, registri IVA, bilanci;
- Dati anagrafici e di identità;
- Dati commerciali, tra i quali comunicazioni da e verso clienti e contatti del Titolare del Trattamento;
- Dati relativi a comunicazioni di servizio;

3EGECO SRL –Sede legale Via Borgonuovo, 27 – 20121 Milano – Sede operativa Via Duca del Mare 19 – 04100 Latina Tel. 0773665876
pec 3egeco@legalmail.it P.iva e C.F. 03097900595 REA MI - 2600871 Capitale sociale deliberato euro 1.000.000,00



- Dati relativi a consensi;
- Dati relativi alla sfera della gestione del personale che contengono presenze paghe, compensi, ritenute, contributi, cartella di medicina del lavoro;
- Dati sanitari.

Durata della conservazione

La conservazione dei dati raccolti è da intendersi per il tempo necessario al compimento della finalità del trattamento e della vigenza dei contratti in essere, comunque non oltre le specifiche prescrizioni in materia di documentazione amministrativa e commerciale, assicurando quindi i tempi previsti dalla normativa quali tempi minimi di conservazione dei dati.

Modalità di conservazione

3EGECO conserva i dati dei propri trattamenti conformemente alle disposizioni normative. I dati vengono conservati secondo principi legati soprattutto alle cautele. Vengono adottate misure di sicurezza al fine di eseguire il trattamento nel rispetto dei principi di riservatezza, integrità, disponibilità ed eliminazione dei dati come esposto più avanti nel presente documento.

La conservazione di dati di trattamenti avviene secondo le modalità successivamente descritte:

- Conservazione cartacea, che prevede tra le altre l'acquisizione di documenti di identificazione, documenti di natura amministrativa, comunicazioni, documenti sanitari, paghe e contributi: ***dal momento della presa in carico sino alla loro eliminazione e/o restituzione.***
- Archiviazione digitale, che prevede tra le altre l'acquisizione di fatture elettroniche, documenti di natura amministrativa, paghe e contributi, documentazione sanitaria, consensi: ***dal momento del caricamento dei dati su sistemi 3EGECO e sino alla loro eliminazione e/o restituzione.***

Le operazioni di modifica parziale, eliminazione e restituzione di dati cartacei e/o digitali vengono certificate da entrambi le Parti attraverso sottoscrizione di specifico verbale.

RAPPORTI CON LA CLIENTELA

Acquisizione del consenso

In ogni proposta progettuale ed economica di 3EGECO che preveda trattamento di dati personali si fa riferimento al presente documento di codice di condotta, di cui l'Interessato può prendere visione.

Le attività di 3EGECO possono prevedere accesso a dati personali e particolari e la liceità del trattamento dei suddetti dati, ovvero la possibilità di accedere ai suddetti dati in ragione del contratto di erogazione di servizi, può essere possibile solo se il Cliente ha fornito consenso al trattamento per le tipologie di dati e relative modalità.

Diritti dell'interessato.



Il Regolamento conferisce all'interessato una serie di diritti che ai sensi delle linee guida sulla trasparenza è obbligatorio riassumere nel loro contenuto principale all'interno dell'informativa. Di seguito tali diritti si riassumono e sintetizzano:

Diritto di accesso (ai soli propri dati personali)

diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che riguardano l'interessato e in tal caso, di ottenere l'accesso ai dati personali e di essere informato su:

- finalità del trattamento;
- categorie di dati personali in questione;
- destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, sul periodo di conservazione dei dati personali previsto oppure, se non è possibile, sui criteri utilizzati per determinare tale periodo;
- qualora i dati non siano stati raccolti presso l'interessato, diritto a ricevere tutte le informazioni disponibili sulla loro origine;
- diritto a ricevere l'informazione sulla esistenza di un processo decisionale automatizzato, compresa la profilazione e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Diritto di rettifica e integrazione

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.

Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto all'oblio ed alla cancellazione

l'interessato ha il diritto di ottenere dal titolare del trattamento l'oblio o la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo (e ove non sussistano le specifiche ragioni dell'art. 17 comma 3 del Regolamento che al contrario sollevano il titolare dall'obbligo di cancellazione) se i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati ed inoltre:

- se l'interessato revoca il consenso e non sussiste altro fondamento giuridico per il trattamento;
- se l'interessato si oppone al trattamento a scopi marketing o profilazione, anche revocando il consenso;

3EGECO SRL –Sede legale Via Borgonuovo, 27 – 20121 Milano – Sede operativa Via Duca del Mare 19 – 04100 Latina Tel. 0773665876
pec 3egeco@legalmail.it P.iva e C.F. 03097900595 REA MI - 2600871 Capitale sociale deliberato euro 1.000.000,00



- se i dati personali sono stati trattati illecitamente o riguardano informazioni raccolte presso minori, in violazione dell'art. 8 del Regolamento.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali cancellazioni salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto alla limitazione del trattamento

l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento (cioè, ai sensi della definizione di “limitazione del trattamento” fornita dall'articolo 4 del Regolamento: “il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro”) quando ricorre una delle seguenti ipotesi:

- l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- l'interessato si è opposto al trattamento marketing, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante. L'interessato che ha ottenuto la limitazione del trattamento è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Diritto di opposizione

l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano svolto dal titolare o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento o svolto per il perseguimento del legittimo interesse del titolare del trattamento o di terzi (ivi inclusa la profilazione).

Inoltre, l'interessato, qualora i dati personali siano trattati per finalità di marketing diretto o di profilazione commerciale, ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità.

Diritto di non essere sottoposto a decisioni automatizzate, compresa la profilazione

3EGECO SRL –Sede legale Via Borgonuovo, 27 – 20121 Milano – Sede operativa Via Duca del Mare 19 – 04100 Latina Tel. 0773665876
pec 3egeco@legalmail.it P.iva e C.F. 03097900595 REA MI - 2600871 Capitale sociale deliberato euro 1.000.000,00



l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, salvo nei casi in cui la decisione automatizzata sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; sia prevista dalla legge, nel rispetto di misure e cautele; si basi sul consenso esplicito dell'interessato.

METODOLOGIE DI PROGETTAZIONE ED IMPLEMENTAZIONE

Valutazione preventiva dell'impatto

Preventivamente alla sottoscrizione di accordi commerciali con i propri Clienti, in caso di gestioni che prevedono trattamento di dati personali, 3EGECO effettua una valutazione di impatto sulla protezione dei dati con l'obiettivo di portare un rischio residuale minimo e accettabile, implementando altresì una politica di miglioramento continuo finalizzata alla riduzione massima del fattore di rischio.

Protezione dei dati cartacei

3EGECO ha predisposto un sistema di immagazzinamento delle informazioni cartacee attraverso locali ed armadi presidiati, chiusi a chiave e dedicati in via esclusiva allo scopo. L'accesso esterno è interdetto ai non autorizzati, è protetto da sistemi anti intrusione ed anti incendio ed è video sorvegliato.

Le informazioni sono contenute in faldoni anonimizzati, le cui etichette non consentono alcuna rilevazione di dati personali in essi contenuti.

I sistemi informatici di gestione della logistica non contengono alcuna informazione di natura personale ma solo indicazioni specifiche del faldone, della provenienza, della posizione in magazzino, della natura dei documenti in esso contenuti.

Protezione dei dati gestiti su sistemi informatici

3EGECO utilizza applicazioni specifiche a supporto dei servizi che eroga alla Clientela.

I sistemi sono progettati avendo particolare attenzione alla gestione della privacy, con piena rispondenza ai principi della privacy by design la quale prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia, dalla primissima fase di progettazione fino alla sua ultima distribuzione, all'utilizzo e all'eliminazione finale.

I sistemi server che ospitano le applicazioni di 3EGECO fornite al Cliente risiedono all'interno della Comunità Europea, ed il Cliente ha diritto in qualsiasi momento di conoscere l'esatta ubicazione delle banche dati oggetto dei servizi sotto contratto.

L'accesso esterno è interdetto ai non autorizzati, è protetto da sistemi anti intrusione ed anti incendio ed è video sorvegliato. I sistemi server non sono utilizzabili quali postazioni di lavoro.

I sistemi server sono dotati di protezione a garanzia della business continuity e sono progettati con l'obiettivo di garantire esercizio 24 ore su 24, sette giorni su sette.

3EGECO SRL –Sede legale Via Borgonuovo, 27 – 20121 Milano – Sede operativa Via Duca del Mare 19 – 04100 Latina Tel. 0773665876
pec 3egeco@legalmail.it P.iva e C.F. 03097900595 REA MI - 2600871 Capitale sociale deliberato euro 1.000.000,00



I sistemi server impiegati da 3EGECO, così come i sistemi client, sono protetti da adeguati sistemi firewall ed IPS e da strumenti anti malware. Le tecnologie sono oggetto di continuo aggiornamento. Le informazioni di natura personale e particolare sono accessibili esclusivamente dietro utilizzo di credenziali caratterizzate da elevato livello di complessità, con policies di rilascio e di accesso che sono convenute direttamente con il Cliente.

3EGeco ha implementato ulteriori misure di sicurezza logica e fisica sugli ambiti informatici e digitali:

- protezione dei dati da accesso non autorizzato agli applicativi;
- protezione dei dati da accesso non autorizzato ai server;
- protezione dei dati da accesso non autorizzato ai database;
- protezione dei dati da accesso non autorizzato alle copie di backup dei database;
- mancanza di opzioni di accesso esterno.

Infine, 3EGECO si avvale di un Responsabile Protezione Dati, che opera sinergicamente con i responsabili interni per l'attuazione delle politiche sulla privacy.

Siti Web

I siti web di 3EGECO hanno scopi di natura informativa ed istituzionale e non operano per acquisire intenzionalmente informazioni sui Visitatori e su abitudini dei Visitatori. Non sono stati attivati strumenti di profilazione. La privacy policy e la cookie policy sono descritte all'interno del sito web in specifiche sezioni, raggiungibili direttamente dalla home page.

E' presente un modulo di raccolta dati per coloro che richiedono informazioni. Il form raccoglie temporaneamente i dati ed invia una mail all'ufficio competente e non viene conservata sul server alcuna ulteriore informazione.

GESTIONE DEI DATA BREACH

3EGeco è fortemente protesa verso il massimo contenimento dei rischi di data breach, interpretando la motivazione più importante che sottintende l'intero impianto normativo del Regolamento Europeo 679/2016.

Con il termine data breach si intende un incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato, a cui segue una notifica della violazione avvenuta. Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'autorità) o ad elevato rischio (per la comunicazione agli interessati) le libertà, la dignità e i diritti degli individui.

Appurato il rischio conseguente dalla violazione, gli articoli 33 e 34 del Regolamento Europeo 679/2016 indicano ai titolari i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di data breach.



3EGECO osserva le disposizioni dell'articolo 33 con il quale si impone al Titolare del trattamento (o ad eventuale Responsabile esterno) di notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza.

Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui si acquisisce consapevolezza dell'avvenuta violazione con un ragionevole grado di certezza in merito alla verifica di un incidente di sicurezza. A titolo esemplificativo, non esaustivo:

- la perdita temporanea di accesso ad un indirizzario e-mail a causa di un blackout non rappresenta evento che richiede una notifica;
- la perdita temporanea di accesso a dati bancari è considerata un evento che pone a rischio (anche elevato) i diritti degli individui e viene gestita ai sensi dei suddetti articoli 33 e 34;
- lo smarrimento di una memoria magnetica contenente dati sensibili criptati indecifrabili da terzi, la cui chiave crittografica non è divulgata non rappresenta evento lesivo nei confronti degli interessati e quindi non obbligatoriamente notificabile;
- lo smarrimento di una memoria magnetica contenente dati sensibili in chiaro, o criptati ma decifrabili da terzi, rappresenta evento lesivo nei confronti degli interessati e quindi obbligatoriamente notificabile.

3EGECO ha attuato ogni misura utile al contenimento del rischio di data breach ed alle conseguenti possibili divulgazioni di dati riservati o confidenziali. Per questo motivo, le policies di sicurezza di 3EGECO prevedono alcune specifiche misure:

- gli Incaricati di 3EGECO non utilizzano memorie magnetiche esterne per attività di test e/o trasferimento di dati;
- gli Incaricati di 3EGECO non duplicano basi dati su notebook personali o aziendali;
- gli Incaricati di 3EGECO autorizzati ad accedere a dati personali e particolari sono adeguatamente formati sui rischi correlati e sottoscrivono stringenti accordi di riservatezza a salvaguardia dei dati di 3EGECO e del Cliente.

Nell'ipotesi di rilevazione di un data breach, la procedura prevista da 3EGECO prevede la seguente prassi:

- viene raccolta la segnalazione di avvenuta violazione;
- il Responsabile Protezione Dati certifica l'avvenuta violazione e comunica in tempo reale l'evento al Titolare del trattamento;
- ove necessario viene prodotta la notifica all'autorità di controllo competente, a norma dell'articolo 55;
- ove non si sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione si comunicherà inizialmente un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti, aggiornando l'Autorità in itinere rispetto ai nuovi riscontri;



- in particolari casi potrà essere effettuata un'unica “notifica aggregata” di tutte le violazioni occorse nel breve periodo di tempo (anche superando le 72 ore);
- si valuta se le misure di cifratura e pseudonomizzazione consentono di considerare inintelligibili i dati oggetto della violazione, escludendo quindi la necessità di comunicazione agli interessati (salvo diverse disposizioni dell’Autorità);
- in caso di rischio elevato per gli interessati, il DPO avvia le procedure di comunicazione dell’avvenuta violazione agli interessati consentendo loro di attivarsi a tutela dei propri interessi, come previsto dall’articolo 34 del Regolamento Europeo 679/2016. La notifica sarà inviata a mezzo email, SMS o con messaggi diretti il cui contenuto è comunicato in maniera evidente e trasparente, con terminologia immediatamente comprensibile;
- se la violazione riguarda dati sanitari, la comunicazione avrà luogo entro 48 ore dalla conoscenza del fatto, indicando le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati;
- si procede con un aggiornamento del documento di valutazione dei rischi e delle misure di contenimento, il cui giudizio prognostico dovrà essere personalizzato avendo riguardo alle concrete circostanze della violazione;
- si attuano misure e correttivi finalizzati all’impedire il verificarsi di analogo data breach.

Per consentire l’attività di accertamento del Garante, verrà predisposto un elenco aggiornato delle violazioni subite, con il dettaglio delle circostanze e delle conseguenze. L’inventario adotterà misure che ne garantiscano integrità ed immodificabilità.

Nell’eventuale notifica di violazione, verranno indicate tutte le informazioni richieste sulla procedura descritta sul link <https://www.garanteprivacy.it/regolamentoue/databreach>.

TRASFERIMENTO DEI DATI

Portabilità dei dati e/o consegna all’interessato come da articolo 20 del Regolamento Europeo 679/2016

I servizi di 3EGeco non contemplano estrazione di dati in forma strutturata da fornire in via diretta all’interessato. Ove fattibile, il processo di estrazione e consegna è comunque eseguito dietro richiesta formale del Titolare del Trattamento. Altresì non è prevista consegna di documentazione cartacea direttamente all’interessato, fatti salvi accordi formali presi direttamente con il Titolare del Trattamento.

Trasferimento a terzi

Nessuna forma di trasferimento e/o di estrazione dei dati a terzi è possibile, fatte salve richieste dell’Autorità o specifiche richieste del Cliente.

FORMAZIONE

Ambito interno



3EGECO organizza piani periodici di formazione dei propri Collaboratori, nel pieno rispetto dei dettami dell'articolo 29 del Regolamento Europeo 679/2016, che stabilisce che “il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare”.

La formazione ha per oggetto aspetti legati alla normativa ed agli aggiornamenti ed adeguamenti, nonché la valutazione di casi pratici, la valutazione delle problematiche correlate ai servizi erogati al Cliente e la presentazione delle procedure interne di compliance.

I Collaboratori di 3EGECO interessati ai trattamenti di dati personali e particolari ricevono specifiche nozioni a seconda dei ruoli da questi ricoperto.

CONTATTI

Per qualsiasi ulteriore chiarimento è possibile rivolgersi al Responsabile Protezione Dati inviando un messaggio e-mail all'indirizzo **privacy@3egeco.it**