FONDAZIONE
Cassa di Risparmio di IMOLA

Modello Organizzativo Privacy

documento approvato con delibera 20.05.2021 del Consiglio Generale

Versione 1.1 del 01/12/21

Redazione documento: Dott. N. Conti
Verifica documento: Dott. G. Vignazia
Approvazione documento: Dott. Lamberto Lambertini

Fondazione Cassa di Risparmio di Imola
Palazzo Sersanti, Piazza Matteotti, 8
44026 Imola (BO)
Tel + 39 0542 26606

C.F. 00467050373
segreteria@fondazionecrimola.it

Indice generale

1 Premessa 4
2 Ambito di applicazione 6
3 Definizioni 7
4 Qualità e conservazione dei dati personali 10
5 Adempimenti 11
6 Responsabilità interna dei trattamenti 12
6.1 Titolare del Trattamento 12
6.2 Delegato alla gestione della privacy 12
6.3 Supporto Consulenziale 12
6.4 Responsabili del Trattamento 12
6.5 Amministratori di sistema 12
6.6 Autorizzati al trattamento 15
7 Trattamenti affidati all'esterno della Ente 16
7.1 Esclusioni dalle operazioni di trattamento 16
8 Dettaglio degli adempimenti 17
8.1 Richiesta di verifica preliminare 18
8.2 Informativa e consenso 18
9 Riscontro delle richieste avanzate ai sensi dell'art. 15 del GDPR 19
10 Designazione degli Autorizzati e ambito di trattamento consentito 20
10.1 Designazione degli Autorizzati interni alla Ente 20
10.2 Modalità di svolgimento delle operazioni 21
10.3 Istruzioni per l'uso degli strumenti di trattamento 21
10.4 Istruzioni in tema di sicurezza 22
11 Misure di sicurezza a protezione dei dati personali 24
11.1 Misure di sicurezza organizzative 24
11.1.1 Minimizzazione dei dati 24
11.1.2 Protezione dell'accesso ai locali 24
11.1.3 Idonee misure di sicurezza in mobilità 25
11.1.4 Composizione robusta e scadenza delle password 25
11.1.5 Idonea custodia delle password 25
11.1.6 Gestione delle violazioni della password 26
11.1.7 Segretezza della password 26
11.1.8 Idoneo smaltimento e consegna in assistenza dei dispositivi elettronici 26
11.1.9 Idonee misure di conservazione e smaltimento della carta 26
11.1.10 Idoneo comportamento durante la navigazione e l'utilizzo della posta elettronica 27
11.1.11 Formazione del personale 27
11.1.12 Procedure ed istruzioni per il personale 27
11.1.12 Impegni ed istruzioni per i fornitori 28
11.2 Misure di sicurezza tecniche 28
11.2.1 Pseudonimizzazione dei dati 28
11.2.2 Cifratura dei dati 28
11.2.3 Software antivirus e anti-malware 29
11.2.4 Software firewall/antintrusione 29
11.2.5 Aggiornamenti di sicurezza del software 30
11.2.6 Idonea gestione degli accessi WiFi 30
11.2.7 Idonea configurazione dell'accesso a internet 30
11.2.8 Firewall/router 30
11.2.9 Backup e disaster recovery 31
11.2.10 Utilizzo del Cloud 32
11.2.11 Profilazione utenti 32
12 Policy per la gestione del "Data Breach" 33

12.1 Definizioni ed identificazione delle violazioni 33
12.1.1 Notifica/Comunicazione *33*
12.1.2 Violazione di dati *33*
12.1.3 Identificazione dell'incidente di sicurezza *34*
12.1.4 Valutazione del livello di criticità della Violazione *36*
12.1.5 Procedura di identificazione e gestione degli incidenti *36*
12.2 Processo di gestione degli incidenti di sicurezza 37
12.2.1 Rilevamento e Segnalazione *38*
12.2.2 Analisi e classificazione *39*
12.2.3 Trattamento *39*
12.2.4 Chiusura Incidente *40*
12.2.5 Follow up e Reporting *40*
Allegati 41

1 Premessa

La Fondazione Cassa di Risparmio di Imola è da sempre particolarmente sensibile alla riservatezza ed alla sicurezza dei dati personali, propri e di terze parti. Per tale motivo ha uniformato il proprio modo di trattare i dati personali ai dettati del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati) (di seguito GDPR o Regolamento Privacy), prevedendo, altresì, misure di sicurezza adeguate a quanto richiesto dalla norma.

La riservatezza delle persone fisiche attraverso la corretta acquisizione, gestione e circolazione dei dati personali e mediante l'adozione di idonee misure di sicurezza per la loro protezione è tutelata dal citato Regolamento, nonché, in quanto non incompatibili, dalle singole normative nazionali e dai provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali.

Il Regolamento afferma importanti principi quali il diritto alla protezione dei dati personali e quello della necessità del trattamento (*need to know*) e, al contempo, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale, al diritto alla protezione dei dati personali, alla portabilità dei dati, sino al diritto all'oblio.

I principi fondamentali introdotti dal Regolamento e non presenti nel precedente "Codice Privacy" (D.Lgs. 196/03), possono essere riassunti come segue:

- *data protection by design* e *data protection by default*;
- Rafforzamento del principio del *need to know*;
- Introduzione di adempimenti formali come l'adozione del Registro dei Trattamenti e redazione del DPIA – *Data Protection Impact Assessment*;
- Nuovi diritti degli interessati;
- Obbligo di gestione dei *Data Breaches*;
- Determinazione delle misure di sicurezza secondo un approccio basato sul rischio;
- Introduzione della figura del DPO – *Data Protection Officer* (Responsabile della Protezione dei Dati Personali);
- Ridefinizione della figura del Responsabile del Trattamento dei Dati Personali e del Contitolare del trattamento;
- Forte inasprimento delle sanzioni che, in caso di inadempimento, possono arrivare sino a € 20 milioni o al 4% del fatturato annuo globale.

Il Regolamento specifica, altresì, che il trattamento dei dati è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il suo esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Il Regolamento si compone di 173 "consideranda" e di 99 articoli.

Il presente documento contiene il Modello Organizzativo definito dalla Fondazione Cassa di Risparmio di Imola (nel seguito, per brevità l' "Ente") per adempiere alle prescrizioni del Regolamento. Esso contiene le indicazioni

per l'effettuazione degli adempimenti necessari verso l'Autorità Garante (quali la notificazione dei trattamenti e dei *Data Breaches*), verso i soggetti interessati (quali l'informativa, la raccolta del consenso al trattamento, laddove necessario, il riscontro delle richieste di esercizio del diritto d'accesso) e verso le strutture operative (quali le nomine e le istruzioni agli Autorizzati ed agli eventuali Responsabili del trattamento ed al Responsabile per la Protezione dei Dati Personali).

2 Ambito di applicazione

Il Regolamento si applica alle attività che comportano il trattamento dei dati personali di titolarità della Fondazione Cassa di Risparmio di Imola (quali, ad es. attività connesse alla gestione del personale, agli organi sociali e agli adempimenti relativi ai propri soci, fornitori ed eventuali consulenti, per cui l'Ente ha titolarità autonoma) ovvero alle attività che comportano il trattamento dei dati personali per le quali l'Ente sia stato individuato, ai sensi dell'art. 28 GDPR, in qualità di responsabile del trattamento (quali, ad es. attività oggetto di contratti di servizio sottoscritti con Pubbliche Amministrazioni ovvero con Associazioni per le quali ha ricevuto apposita nomina) nel rispetto delle finalità determinate dalle controparti e secondo le modalità previste dal contratto di servizio e dalla nomina ricevuta.

Le nomine dell'Ente in qualità di responsabile del trattamento definiscono l'ambito del trattamento autorizzato da parte dei soggetti titolari del trattamento. Nessun trattamento ulteriore è consentito, se non previa autorizzazione dei titolari a cui compete in via esclusiva la verifica della compatibilità dei trattamenti effettuati rispetto alle informative rilasciate ex art. 13 del Regolamento UE ed ai consensi acquisiti dagli interessati, o ex art. 14 del medesimo Regolamento se i dati non siano stati ottenuto presso l'interessato.

3 Definizioni

Preliminarmente, al fine di una corretta interpretazione degli adempimenti che saranno menzionati nel seguito, si fornisce un'esplicitazione dei termini utilizzati nel Regolamento.

In particolare, si intende per:

1. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un dato come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4. Privacy by Design e Privacy by Default: l'art. 25 del GDPR prevede in capo al Titolare del Trattamento due modalità di gestione del Modello Organizzativo Privacy interno del proprio Ente. La prima, prevista al comma 1 dell'art. 25 è definita privacy by Design poiché il compito del Titolare sarà quello di adottare e attuare misure tecniche organizzative che tutelano i principi di protezione dei dati sin dal momento della progettazione. Differente è invece la Privacy by Default (art. 25 comma 2), il cui principio è quello di garantire che vengano trattati per impostazione predefinita solo i dati necessari per ogni specifica finalità del trattamento, garantendo in questo modo automaticamente il principio di minimizzazione dei dati;

5. «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

6. «pseudonimizzazione»: il trattamento dei dati personali in modo tale che tali dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

7. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

8. «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

9. «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

10. «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri (4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT) non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

11. "Responsabile della Protezione dei Dati Personali": noto con l'acronimo inglese DPO (Data Protection Officer), è la figura prevista e normata dagli artt. 37, 38 e 39 del Regolamento il cui compito precipuo è quello di monitorare il rispetto della normativa; fungere da *trait d'union* tra l'Ente ed il Garante; informare e fornire consulenza al titolare, al responsabile e/o ai dipendenti in ordine agli obblighi previsti dal Regolamento; fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

12. «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

13. «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

14. «violazione dei dati personali» (Data Breach): la violazione 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;

15. «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

16. «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

17. «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18. «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le Ente di persone o le associazioni che esercitano regolarmente un'attività economica;

19. «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; (4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT);

20. «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà

fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

4 Qualità e conservazione dei dati personali

I dati personali devono essere:

- esatti ed aggiornati;
- trattati unicamente per gli scopi determinati, espliciti e legittimi definiti dalla Ente;
- pertinenti, completi e non eccedenti rispetto alle finalità della raccolta.

I sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. All'uopo sono utilizzate opportune clausole contrattuali, seguendo le procedure interne, le indicazioni del titolare e le indicazioni in termini di legge, quando lo sviluppo del software è commissionato all'esterno dell'Ente. I dati personali da questa trattati sono conservati per il tempo necessario al raggiungimento delle finalità specificate nelle informative per le diverse categorie di soggetti, dopodiché vengono cancellati seguendo le procedure interne e le prescrizioni di legge.

5 Adempimenti

Nomina del DPO: il Responsabile della Protezione dei dati deve essere nominato obbligatoriamente nei casi in cui, ex art. 37 del GDPR, le attività principali del Titolare consistano in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala; e tali attività consistano nel trattamento, su larga scala, di categorie particolari di dati. La Fondazione Cassa di Risparmio di Imola alla data di approvazione del presente Modello Organizzativo non ha individuato né nominato un DPO in quanto, alla luce delle analisi svolte, non si applicano le fattispecie ex art. 37 GDPR. Tuttavia la decisione è sottoposta a continue e successive valutazioni, anche in capo ad una eventuale nomina su base volontaria.

Notificazione dei *Data Breaches*: ogni qual volta si verifichi un attacco informatico, una perdita, una manomissione o un accesso abusivo dei dati personali trattati il Titolare o, quando necessario, il Responsabile della Protezione dei dati deve avvertire l'Autorità di Controllo entro 72 ore dalla scoperta (art. 33). La notifica deve contenere le caratteristiche della violazione; il numero degli interessati coinvolti; i contatti interni dell'operatore ed una stima delle conseguenze. Nel caso in cui tale violazione metta a rischio i diritti e le libertà degli interessati il Titolare dovrà, con un linguaggio semplice, informarli di quanto accaduto e delle misure adottare per affrontare la violazione.

Informare i soggetti interessati: Per questo gruppo di adempimenti sono considerate le categorie di soggetti interessati rappresentate dalle terze parti, persone fisiche, i cui dati sono trattati dal'Ente. Sono altresì prese in considerazione le specifiche situazioni relative alla videosorveglianza con registrazione immagini, e ai trattamenti effettuati attraverso il sito internet.

Designare, formare e istruire gli autorizzati al trattamento: l'Autorizzato del Trattamento è la persona fisica autorizzata dal Titolare o dal Responsabile a compiere le operazioni di trattamento dei dati. Avendo il compito di effettuare materialmente le operazioni di trattamento sui dati personali, egli deve agire sotto la diretta autorità del titolare del trattamento. Gli autorizzati sono nominati con apposito atto a firma del Legale Rappresentante.

Nominare e fornire istruzioni ai Responsabili del Trattamento: elaborano i dati personali per conto del Titolare del trattamento nel pieno rispetto delle disposizioni in materia di protezione dei dati e delle linee guida del Titolare. La nomina a Responsabile del trattamento ex art. 28 del GDPR spetta al legale rappresentante della Ente.

Nominare e istruire gli amministratori di sistema: l'amministratore di sistema o, tecnico sistemista di rete, è una figura professionale che approfondisce le competenze di un tecnico hardware e software soprattutto per quanto riguarda le caratteristiche delle architetture informatiche, i livelli di sistemistica e, in particolare, l'utilizzo e la condivisione di grandi quantità di dati attraverso le reti di comunicazione.

6 Responsabilità interna dei trattamenti

L'Ente, in qualità di Titolare del trattamento di dati personali, ha individuato la propria struttura di presidio della data protection che fa capo alla Segreteria Generale, come precisato al successivo punto 6.2.

6.1 Titolare del Trattamento

Il Titolare del trattamento ai sensi dell'art. 4, c.1, n. 8 del Regolamento europeo 2016/679 è l'Ente nel suo complesso, che è attualmente rappresentata dal Legale Rappresentante pro tempore.

6.2 Delegato alla gestione della privacy

Viene delegata l'organizzazione interna della tutela della privacy, con la facoltà di nominare quale Delegato interno all'Ente nell'ambito delle rispettive competenze, per la verifica delle procedure e della compliance in tema di protezione dei dati, il Dott. Giovanni Vignazia, responsabile dell'Ufficio Organizzazione.

Il Delegato alla gestione della privacy ha la competenza esclusiva del riscontro rispetto alle richieste - da chiunque pervenute anche ai sensi dell'art. 15 del GDPR - di accesso, ovvero estrazione di dati di titolarità della Fondazione Cassa di Risparmio di Imola.

6.3 Supporto Consulenziale

Il Delegato può essere su specifica richiesta supportato da un consulente esterno nelle attività delegate di organizzazione e gestione della privacy dell'Ente. La Funzione coordina la gestione operativa degli adempimenti in materia di privacy, effettua l'istruttoria sulle richieste di accesso o estrazione dati provenienti da soggetti terzi (ad esempio per indagini di polizia giudiziaria ovvero per istanze di accesso ai sensi dell'art. 15 e ss. del Regolamento); cura gli approfondimenti normativi e verifica, con la collaborazione dei Responsabili degli uffici dell'Ente, l'applicazione del presente regolamento e di ogni ulteriore disposizione dell'Ente in materia di privacy, ivi inclusa la corretta preposizione di Autorizzati ed addetti alla manutenzione nonché l'aggiornamento delle credenziali assegnate a ciascun preposto per l'accesso agli strumenti elettronici di trattamento dei dati effettuate a cura dell'Amministratore di sistema (vedere par. 1.6.5).

6.4 Responsabili del Trattamento

Ai sensi dell'art. 28 del Regolamento, i soggetti esterni che, in qualità di fornitori, consulenti o comunque contraenti, per esigenze organizzative dell'Ente, gestiscono specifici servizi o svolgono attività connesse, strumentali o di supporto a quelle dell'Ente e che pertanto effettuano attività di trattamento di dati personali di titolarità dell'Ente (ad es.: fornitura di prestazioni professionali o di prestazioni e servizi anche in convenzione quali consulenti, istituti di credito ed assicurativi, ecc.), sono di norma individuati in qualità di Responsabili del trattamento, sempre che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento. In alternativa, ovvero nel caso i cui i fornitori/consulenti trattino dati di titolarità dei soci/committenti della Fondazione Cassa di Risparmio di Imola dovrà essere richiesto l'elenco nominativo delle persone fisiche preposte dai fornitori/consulenti alle attività che comportano il trattamento di dati personali e copia delle relative istruzioni operative impartite ai fini delle necessarie verifiche ed integrazioni da parte dell'Ente.

6.5 Amministratori di sistema

L'Ente individua l'Amministratore di Sistema – cui affidare gli adempimenti in materia di sicurezza indicati dal Regolamento all'art. 32 – in assenza di personale interno dotato di competenze tecniche in ottemperanza al Provvedimento del Garante recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema del 27 novembre

2008" (G.U. n. 300 del 24 dicembre 2008), come modificato ed integrato dal successivo provvedimento del 25 giugno 2009.

Sulla base di tale valutazione, alla data di redazione del presente documento, è stato individuato il fornitore di Servizi ICT DZ GHROUP S.r.l. DZ Group S.r.l. quale Amministratore di sistema - con atto di nomina a Responsabile del Trattamento dati con funzioni di Amministratore di Sistema - contenente l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato – i cui estremi identificativi, unitamente all'elenco delle funzioni ad essi attribuite, sono riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte dell'Autorità Garante.

Compiti ed attribuzioni dell'Amministratore di sistema (con attività differenziate a seconda del profilo proprio dell'Amministratore di sistema e dei compiti attribuiti):

a) gestire le credenziali di autenticazione dei responsabili e dei soggetti autorizzati al trattamento/addetti alla manutenzione;

b) gestire i profili di autorizzazione degli autorizzati al trattamento dei dati/addetti alla manutenzione, su specifiche indicazioni impartite dai responsabili del trattamento;

c) provvedere alla disattivazione/variazione delle utenze assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili;

d) pianificare la formazione del personale tecnico, in materia di soluzioni tecniche per la garanzia della sicurezza dei dati e della protezione degli strumenti elettronici;

e) custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali.

Compiti da gestire direttamente ovvero anche tramite addetti alla manutenzione e gestione degli strumenti elettronici:

a) adottare i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al loro ricovero periodico con copie di back-up secondo i criteri stabiliti;

b) assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

c) prevedere procedure operative per la disattivazione dei "codici identificativi personali" (User-ID), in caso di perdita della qualità di autorizzato all'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei "codici identificativi personali" (User-ID) per un periodo superiore a 3 mesi;

d) proteggere gli strumenti elettronici dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di programmi virus mediante idonee misure di sicurezza da aggiornare almeno ogni 6 mesi;

e) mantenere un adeguato sistema di autorizzazione che, per ogni identificativo utente, riporti la data di attivazione, le funzioni del sistema alle quali l'utente è abilitato, la data di cessazione dell'identificativo stesso;

f) provvedere al salvataggio dei dati presenti sui server e al loro ripristino in caso di necessità;

g) conservare le copie di back-up;

h) registrare e archiviare tutte le attività eseguite sul sistema;

i) garantire che le informazioni scambiate con soggetti interni ed esterni siano opportunamente protette da rischi di intrusione.

Funzioni di controllo e vigilanza nei confronti di fornitori di strumenti elettronici e di addetti esterni alla gestione e manutenzione di strumenti elettronici:

a) l'hardware sia conforme alla normativa in materia di protezione dei dati personali;

b) in occasione di ciascun intervento di manutenzione e di assistenza tecnica, sottoscrivano un verbale sulla esecuzione dei lavori, che attesti la conformità alle regole dette;

c) i software operativi e i programmi applicativi siano idonei ad assicurare:

   - la separazione tra dati anagrafici e dati sensibili, ovvero la cifratura dei dati idonei a rivelare lo stato di salute;
   - la tracciabilità delle attività degli utenti, nel rispetto del Regolamento UE 2016/679 e delle garanzie di tutela dei dipendenti;
   - un sistema di autenticazione e di autorizzazione conforme alla normativa in materia di protezione dei dati personali;

d) i fornitori di piattaforme di data base debbono garantire la tracciabilità delle transazioni degli utenti.

Funzioni di controllo e di vigilanza da attuare al fine di una corretta gestione della privacy dell'Ente (Responsabile di Ufficio):

a) verificare l'adozione delle misure adeguate di sicurezza;

b) verificare lo stato di adozione delle misure idonee di sicurezza;

c) pianificare regolari controlli della vulnerabilità dei programmi per elaboratore;

d) verificare gli eventi che hanno causato rischi per l'integrità e la disponibilità dei dati personali;

e) pianificare attività di audit interno, finalizzata al controllo del rispetto delle istruzioni operative e delle misure di sicurezza;

f) verificare il rispetto delle istruzioni impartite ai responsabili e agli autorizzati al trattamento/addetti alla manutenzione;

g) verificare la congruità delle misure di sicurezza organizzative, fisiche e logiche ad oggi esistenti, e perseguire l'obiettivo di raggiungere un livello di protezione idoneo con particolare riferimento alle recenti disposizioni in materia di trattamento e protezione di dati personali ai sensi del Regolamento UE 2016/679;

h) comunicare a tutti gli autorizzati al trattamento /addetti alla manutenzione le misure da predisporre e/o rispettare per la protezione dei dati di loro competenza, ponendo in essere tutte quelle forme di controllo nel tempo che si riterranno opportune, previa comunicazione per approvazione al Titolare;

i) monitorare lo stato delle misure di sicurezza utilizzando apposita check-list;

j) redigere apposita relazione scritta sulla gestione delle attività assegnate, con particolare riferimento alle misure di sicurezza adottate, alle verifiche periodiche sulla corretta assegnazione delle credenziali di autorizzati/addetti, al conseguente eventuale aggiornamento dei profili attivi e, più in generale, sullo stato della sicurezza informatica dell'Ente.

L'Amministratore di Sistema predispone annualmente per l'Ente apposita relazione in merito alle misure di sicurezza adottate, alle verifiche periodiche sulla corretta assegnazione delle credenziali di Autorizzati/addetti, al

conseguente eventuale aggiornamento dei profili attivi e, più in generale, sullo stato della sicurezza informatica dell'Ente.

6.6 Autorizzati al trattamento

Gli autorizzati al trattamento sono i soggetti – nominati dal Titolare e/o dal Responsabile del trattamento (Art. 29 del Regolamento) – che trattano i dati personali cui hanno accesso, attenendosi alle istruzioni loro impartite dal Titolare e/o dal Responsabile.

Le risorse impiegate in mansioni che comportino trattamento di dati personali devono essere appositamente preposte con nomina sottoscritta dal Segretario Generale; i nominativi degli Autorizzati al trattamento sono forniti al Delegato Privacy, in accordo con il Segretario Generale, unitamente all'indicazione dell'ambito del trattamento.

7 Trattamenti affidati all'esterno della Ente

Ricadono in questa fattispecie le esternalizzazioni di attività dell'Ente che comportano il trattamento di dati personali di cui l'Ente risulti essere Titolare del trattamento. È importante considerare che in tali situazioni deve essere prestata particolare attenzione al rapporto che si instaura con il destinatario dei dati. Nel caso in cui il destinatario sia un *outsourcer* di servizi, la normativa sulla privacy evidenzia obblighi specifici di controllo da parte del Titolare su tali trattamenti. Nel caso di designazione della Società esterna quale responsabile del trattamento è richiesta, ad esempio, una fase propedeutica di valutazione dell'affidabilità del soggetto[1], la resa di specifiche istruzioni[2] ed il controllo dell'operato dell'outsourcer[3].

7.1 Esclusioni dalle operazioni di trattamento

Gli addetti alle pulizie appartenenti ad altre aziende, che, per necessità operative, accedono ai locali della Ente, non sono autorizzati a svolgere alcuna operazione di trattamento. Gli autorizzati adottano comportamenti atti ad evitare che ai trattamenti da loro svolti accedano, pur se accidentalmente, le persone non autorizzate.

1 Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

2 I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

3 Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

8 Dettaglio degli adempimenti

Le seguenti prescrizioni sono da intendersi vincolanti per i dipendenti dell'Ente che siano preposti in qualità di autorizzati del trattamento/addetti alla manutenzione e gestione.

L'eventuale violazione delle disposizioni di seguito riportate costituisce un illecito, che può comportare l'applicazione di sanzioni di natura disciplinare ma anche di natura amministrativa e penale, secondo quanto previsto dal Regolamento 679/2016 e dal Codice Privacy integrato con le modifiche del D. Lgs. 101/2018 recante *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*. Si ricorda, inoltre, che è stato siglato un protocollo d'intesa tra la Guardia di Finanza e l'Autorità Garante per la protezione dei dati personali per una sempre più intesa ed efficace attività di controllo sulla raccolta dei dati. Si auspica una responsabile e consapevole collaborazione da parte di tutti gli autorizzati nella diligente osservanza delle disposizioni di legge e nelle prescrizioni contemplate all'interno del presente modello ai fini di un corretto trattamento dei dati personali e tutela della privacy.

1. Ciascun autorizzato è tenuto a rispettare i principi generali previsti dal Regolamento 679/2016, con particolare riferimento alla liceità e correttezza del proprio agire: l'autorizzato può lecitamente effettuare le operazioni di trattamento secondo le modalità e le finalità espressamente stabilite per ciascun ambito di trattamento, giusta espressa preposizione per iscritto.

2. Il trattamento di dati personali deve essere effettuato in misura pertinente e non eccedente, esclusivamente per le finalità per le quali i dati sono stati raccolti e nella misura in cui queste sono state oggetto di apposita informativa fornita agli autorizzati, come previsto dagli artt. 5-6 del Regolamento 2016/679.

3. Il trattamento di dati personali non deve essere effettuato, qualora sia possibile realizzare le finalità per cui è attuato, attraverso l'uso di dati anonimi.

4. Le attività di trattamento dei dati personali e sensibili (ora "particolari" ex art. 9 del GDPR) devono essere limitate al tempo strettamente necessario al raggiungimento degli scopi per cui i dati medesimi sono stati raccolti o sono successivamente trattati.

5. A seguito della preposizione alla relativa unità di trattamento/manutenzione, ed in relazione alle operazioni consentite secondo il profilo di attività assegnato, ciascun autorizzato/addetto alla manutenzione è dotato di credenziali di autenticazione (user id + password ovvero dispositivi *smart card*) riservate e personali che consentono di accedere ai dati personali che è autorizzato a trattare, nonché ad utilizzare gli strumenti dell'Ente necessari per il trattamento. Le credenziali vengono disattivate al momento della cessazione del rapporto di lavoro, previa comunicazione all'Amministratore di Sistema da parte dell'ufficio risorse umane, ovvero aggiornate, su richiesta dei responsabili, in caso di preposizione ad altra unità di trattamento o di modifica dell'ambito di trattamento consentito.

6. Ciascun soggetto autorizzato allo svolgimento delle operazioni di trattamento ha l'obbligo di mantenere il segreto sui dati raccolti o di cui venga a conoscenza nel corso della propria attività lavorativa, evitando di diffonderli o di comunicarli a terzi o comunque a soggetti non legittimati al trattamento di tali informazioni. Non è pertanto autorizzato a fornire riscontro diretto a richieste, verbali o scritte, di estrazione o di comunicazione di dati di titolarità dell'Ente ovvero di titolarità di terzi, anche qualora tali richieste pervengano da uffici o strutture dell'Ente se non autorizzate all'accesso ai dati medesimi. Di tali richieste dovrà essere data apposita informativa alla Segreteria Generale ai fini delle necessarie verifiche e dell'eventuale formalizzazione del riscontro. In caso di allontanamento dal proprio ufficio o dalla propria

postazione di lavoro, ciascun soggetto preposto allo svolgimento delle operazioni di trattamento deve adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza o non specificamente autorizzato.

7. Qualora l'autorizzato utilizzi, nello svolgimento delle proprie mansioni, atti/documenti contenenti dati personali comuni o particolari, questi non devono essere lasciati incustoditi, ma occorre siano evitati eventuali accessi o la conoscenza da parte di soggetti non autorizzati; alla fine del ciclo di lavoro, la documentazione deve essere sempre riposta negli archivi ad accesso controllato.
8. Al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione delle anagrafiche e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento.
9. I preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzino strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli.

8.1 Richiesta di verifica preliminare

Il trattamento dei dati diversi da quelli particolari (art. 9) e quelli relativi a condanne penali e reati (art. 10) che presenta rischi specifici per i diritti e le libertà fondamentali è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato che sono prescritti dal Garante nell'ambito di una verifica preliminare anche a seguito di una richiesta del Titolare.

La verifica preliminare è da richiedere, ad esempio, per l'uso di sistemi di videosorveglianza c.d. "intelligenti", che non si limitano a riprendere e registrare le immagini, ma sono in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli.

8.2 Informativa e consenso

Solo ed esclusivamente per i dati di cui Fondazione Cassa di Risparmio di Imola risulti Titolare, all'atto della raccolta dei dati vi è l'obbligo di rendere l'informativa ai soggetti interessati e di raccogliere il consenso, ove necessario. L'Ente, di norma, acquisisce il consenso in forma scritta mediante apposita modulistica.

In conseguenza di quanto sopra, il trattamento dei dati personali può essere effettuato esclusivamente per le finalità riportate nelle informative suddette e, nel caso di necessità di consenso, solo per quelle finalità per le quali è stato rilasciato il consenso dagli interessati in conformità all'art. 7 del GDPR: è vietato qualsiasi altro utilizzo non esplicitamente compreso in tale consenso.

9 Riscontro delle richieste avanzate ai sensi dell'art. 15 del GDPR

Il Regolamento tutela l'Interessato riservandogli, tra l'altro, specifici diritti (artt. da 15 a 22 del GDPR) in merito al trattamento ed al diritto di accesso ai propri dati personali e, in particolare, consentendo di ottenere dal Titolare, dal Responsabile, se designato, e/o dal DPO:

a) la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, la loro comunicazione in forma intelligibile nonché l'indicazione della loro origine, delle finalità e delle modalità del trattamento, della logica applicata in caso di trattamenti effettuati con l'ausilio di mezzi elettronici, degli estremi identificativi del Titolare, del Responsabile dei Trattamenti, del Responsabile della Protezione dei Dati Personali e del Rappresentante del Titolare, se designato, dei soggetti o delle categorie di soggetti che possono venirne a conoscenza dei propri dati personali;

b) l'aggiornamento, la rettifica, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati e l'attestazione che queste ultime operazioni (dall'aggiornamento al blocco) sono state portate a conoscenza di coloro ai quali i dati sono stati comunicati o diffusi; di opporsi in tutto o in parte per legittimi motivi al trattamento di dati personali che lo riguardano anche quando questo è previsto a fini di informazioni commerciali o di invio di materiale pubblicitario o di vendita diretta ovvero per il compimento di ricerche di mercato o di comunicazione commerciale.

L'interessato, inoltre, ha il diritto di proporre reclamo all'Autorità di Controllo.

Il riscontro alla richiesta dell'Interessato, ai sensi dell'art. 15 del Regolamento ("Diritto di accesso dell'Interessato"), deve essere effettuato dal Titolare o dal Responsabile.

Per l'esercizio dei suddetti diritti da parte dell'interessato l'Ente mette a disposizione un contatto dedicato, oltre al *template* formulato dal Garante della Protezione dei Dati Personali.

10 Designazione degli Autorizzati e ambito di trattamento consentito

La nomina degli autorizzati è un adempimento fondamentale per il trattamento dei dati personali sia in caso di utilizzo di strumenti elettronici[4] sia nel caso di trattamenti effettuati senza l'ausilio di essi[5].

Gli Autorizzati sono nominati dall'Ente, tramite una lettera di nomina:

- nel caso di nuovo dipendente, all'atto dell'assunzione o della specifica lettera di incarico alla mansione;
- nel caso di collaboratore esterno, all'inizio del rapporto di collaborazione;
- nel caso di *stagiaire*, all'inizio dello *stage*.

In tutti i suddetti casi la nomina ad autorizzato, corredata da specifiche istruzioni per l'ambito di trattamento assegnato, viene controfirmata in calce dal soggetto designato per ricevuta ed integrale presa visione.

10.1 Designazione degli Autorizzati interni alla Ente

Il personale dipendente in servizio presso l'Ente è autorizzato a trattare i dati personali, di cui l'Ente stesso è Titolare o Responsabile, strettamente necessari e/o comunque connessi alle funzioni proprie dell'unità organizzativa di appartenenza alla quale il singolo autorizzato è addetto. Tale trattamento può essere effettuato attraverso l'accesso agli archivi cartacei a disposizione della predetta unità organizzativa e l'utilizzo delle procedure informatiche previsto dal profilo di abilitazione assegnato.

I dati personali particolari e relativi a condanne penali, potranno essere trattati, nel rispetto delle Autorizzazioni generali emanate dall'Autorità Garante (in particolare le Autorizzazioni n. 1, 5 e 7) e reperibili sul sito della stessa Autorità, dalle seguenti categorie di autorizzati dell'Ente:

- per quanto riguarda i dati inerenti al rapporto di lavoro dei dipendenti e assimilati e dei loro familiari: dagli addetti dell'Amministrazione, nonché dai diretti superiori;
- dati dei fornitori (che vengono acquisiti da Uffici/Enti certificatori Terzi e non dall'interessato): dall'ufficio approvvigionamenti e legale.

Taluni autorizzati al trattamento di dati particolari e relativi a condanne penali o reati potranno ricevere ulteriori specifiche indicazioni che integrano quelle generali di cui al presente Modello Organizzativo. I responsabili degli uffici verificano periodicamente la pertinenza, non eccedenza e indispensabilità dei dati particolari e relativi a condanne penali o reati trattati presso le funzioni di competenza.

Inoltre, per quanto riguarda il personale addetto dell'Amministrazione, in funzione del ruolo ricoperto, è consentito l'accesso ai dati di diversa natura (particolari, relativi a condanne penali, di rischio specifico), necessari allo svolgimento di detto ruolo.

In particolare, ciascun autorizzato del trattamento deve:

- rispettare i principi generali previsti dal Regolamento 2016/679, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, comunque connessi alla *mission* e all'ambito di operatività assegnato. Si

4 "Il trattamento di dati personali con strumenti elettronici è consentito agli autorizzati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti."

5 Agli autorizzati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali".

ricorda, altresì, che i dati devono essere trattati nei limiti della pertinenza, completezza e non eccedenza rispetto alle finalità per cui sono raccolti o successivamente trattati;

- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'Ente.

L'autorizzato, inoltre, deve:

- rispettare le misure adeguate di sicurezza adottate dall'Ente, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze.

10.2 Modalità di svolgimento delle operazioni

- Identificazione dell'autorizzato: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- verifica del controllo dell'esattezza del dato e della corretta digitazione: al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'autorizzato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;
- accesso fisico ai locali: i locali, ove sono custoditi i dati personali (ed in particolare quelli di natura particolare), devono essere soggetti a controllo e a verifica, al fine di evitare che, durante l'orario di lavoro, possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza.

10.3 Istruzioni per l'uso degli strumenti di trattamento

- Strumenti elettronici: ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card, etc). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità

giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato;

- posta elettronica: l'uso della posta elettronica è autorizzato esclusivamente per finalità di lavoro, per cui si raccomanda di non inviare comunicazioni a soggetti estranei agli scopi istituzionali o professionali. Si informa che, in caso di assenza prolungata, può essere richiesto all'autorizzato di individuare un proprio fiduciario autorizzato ad accedere alla casella assegnata dal titolare o dal responsabile del trattamento. Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari, si raccomanda di prestare attenzione a che:
  - l'indirizzo del destinatario sia stato correttamente digitato;
  - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura particolare;
  - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;
- distruzione delle copie cartacee: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzino strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;
- atti e documenti cartacei: gli atti e i documenti, contenenti dati personali o sensibili, non devono essere lasciati incustoditi; occorre che gli autorizzati, cui sono affidati per lo svolgimento delle loro mansioni, controllino eventuali accessi o la conoscenza da parte di soggetti non autorizzati. Alla fine del ciclo di lavoro, la documentazione deve essere riposta negli archivi ad accesso controllato.

10.4 Istruzioni in tema di sicurezza

- Accessi a strumenti elettronici mediante utilizzo di credenziali di autenticazione: la parola chiave, assegnata a ciascun autorizzato da parte della Fondazione Cassa di Risparmio di Imola, è composta da un numero di caratteri almeno pari a otto o comunque pari al numero massimo di caratteri consentito dal sistema. Ciascun autorizzato, nel gestire la propria password deve:
  - provvedere alla sostituzione immediata della password assegnata, secondo le modalità operative previste dal sistema, e successivamente cambiare la propria credenziale con cadenza almeno trimestrale;
  - nel procedere alla sostituzione e al cambio periodico, ciascun autorizzato deve adottare una password di lunghezza almeno pari a quella che gli è stata precedentemente assegnata;
  - scegliere una password che non deve contenere riferimenti agevolmente riconducibili alla sfera personale o all'identità dell'autorizzato medesimo;
  - evitare di divulgare o comunicare a terzi la password che deve essere segreta e non lasciata incustodita, con avvertimento che ogni accesso a strumenti elettronici mediante utilizzo della componente riservata della credenziale assegnata è imputabile al soggetto che ne risulta titolare, con conseguente onere e obbligo di provare l'uso indebito e non autorizzato;

- back-up: salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, per le finalità di cui in premessa, utilizzando gli apparati eventualmente messi a disposizione da parte di Fondazione Cassa di Risparmio di Imola;
- antivirus: a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati devono procedere all'effettuazione delle operazioni di aggiornamento, di volta in volta richieste dal sistema, secondo le istruzioni visualizzate sullo schermo;
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, adottare misure atte a escludere che soggetti non autorizzati possano acquisire informazioni o accedere alle banche dati gestite. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero uscire dal programma che si sta utilizzando, ove sia protetto da parola chiave, ovvero, in alternativa, spegnere l'elaboratore che si sta utilizzando.

11 Misure di sicurezza a protezione dei dati personali

La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate a garantire il rispetto delle disposizioni del Regolamento (art. 32).

Al fine di poter dimostrare la conformità con il Regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita.

Le misure di sicurezza mitigano, per loro natura, il rischio sul trattamento dei dati personali, agendo:

- sulla gravità dell'evento temuto, riducendo ad esempio l'identificabilità o gli effetti pregiudizievoli sull'interessato;
- sulla probabilità che la minaccia si concretizzi nell'evento temuto, riducendo ad esempio le vulnerabilità degli asset di ausilio ai trattamenti;

e in relazione ai seguenti eventi temuti:

- divulgazione non autorizzata o accesso a dati personali,
- modifica non autorizzata di dati personali o di trattamenti,
- distruzione o perdita di dati personali o indisponibilità di trattamenti.

Nello scenario moderno, assume sempre maggior importanza il trattamento dei dati mediante strumenti informatici e tecnologici. L'utilizzo di tali strumenti ha introdotto nuove tipologie di vulnerabilità per i dati in essi contenuti. La maggior parte delle vulnerabilità informatiche, è innescata da errati comportamenti, o mancata applicazione di adeguate misure di sicurezza, molto spesso, a causa della scarsa conoscenza dei rischi e delle contromisure. Nel seguito vengono illustrate, brevemente, le misure più comunemente consigliate, per aumentare il livello di protezione dei dati contenuti in supporti digitali e cartacei e trattati con strumenti informatici e non.

11.1 Misure di sicurezza organizzative

11.1.1 Minimizzazione dei dati

La limitazione della raccolta delle categorie e della quantità di dati personali trattati a quanto necessario alla finalità del trattamento, non solo è un principio fondamentale del Regolamento, ma è anche una misura di sicurezza volta a ridurre l'identificabilità dell'interessato e gli effetti pregiudizievoli sull'interessato stesso, ovvero la gravità del rischio sui trattamenti.

11.1.2 Protezione dell'accesso ai locali

Evidente come la protezione dell'accesso ai locali sia una misura indispensabile per i supporti cartacei, meno evidente il fatto che costituisce una misura di sicurezza anche per i dispositivi elettronici. È molto più facile compromettere un dispositivo, quando se ne ha l'accesso fisico. Gli attacchi mediante intrusione informatica, oltre ad essere molto complessi, in presenza di adeguati dispositivi di sicurezza, hanno lo svantaggio di essere "online". Se occorre molto tempo, è probabile che qualcuno se ne accorga e ponga fine ai tentativi. Viceversa, se un malintenzionato riesce ad appropriarsi di un dispositivo, avrà tutto il tempo che desidera per tentare di violarlo e prendere possesso dei dati in esso contenuti. Per questo, la protezione fisica dei locali contenenti dispositivi informatici è altrettanto e forse anche più importante di quella dei locali contenenti archivi cartacei. Sottrarre un singolo hard disk potrebbe equivalere a sottrarre migliaia di faldoni. I locali che ospitano server, dovrebbero sempre essere dotati di misure di sicurezza, e gli accessi consentiti solo al personale addetto e fidato. Sarebbe

anche bene che fossero, logisticamente, in posizioni centrali, difficilmente accessibili con la semplice infrazione, per esempio, di una porta o di una finestra.

11.1.3 Idonee misure di sicurezza in mobilità

Quando si trasportano documenti cartacei, ma anche dispositivi contenenti dati, o, comunque, in grado di accedere direttamente ai dati, occorre tenere conto che i rischi aumentano notevolmente. A parte l'ovvio rischio di sottrazione del dispositivo, bisogna anche tenere conto della possibilità di caduta, con conseguente guasto. Possono anche sussistere condizioni che mettano a rischio l'integrità del dispositivo, come temperature molto alte (es. auto al sole) o molto rigide, oppure forti campi elettromagnetici (es. scanner al check in aereo). Tutti questi rischi possono essere mitigati in 2 fasi. Innanzitutto, è necessario disporre sempre di una copia dei dati in un luogo "fisso" sicuro, contro il rischio di guasti. Poi è bene rendere inservibili i dati in caso di furto del dispositivo. Questo è possibile mediante la cifratura, già vista nel caso dei backup, ma che, nel caso di dati "correnti", ha delle implicazioni un po' diverse, che analizzeremo nei prossimi paragrafi.

Un altro aspetto a cui prestare molta attenzione, quando si è in mobilità, è l'accesso a reti WiFi sconosciute. Attraverso queste reti, noi possiamo accedere a dati dell'Ente, pubblicati attraverso Internet, ma siamo vulnerabili a intercettazioni di dati e password a nostra insaputa. Parlando del *cloud* vedremo che esistono metodi per scongiurare questa possibilità.

11.1.4 Composizione robusta e scadenza delle password

Le password sono un elemento di sicurezza fondamentale. Oltre a permettere l'accesso ai sistemi operativi, ai software o ai portali di trattamento dei dati, possono concorrere anche alla cifratura dei dati. Chi viene in possesso di un dispositivo e della relativa password, ha l'accesso completo al contenuto di quel dispositivo. Per questo è importante che le password sia "robuste".

Esistono numerosi software in grado di "indovinare" le password e, tendenzialmente, utilizzano metodologie di attacco con forza bruta: cioè la prova ripetuta di combinazioni casuali di caratteri, che, con dispositivi opportuni, possono arrivare anche al ritmo di migliaia di miliardi di tentativi al secondo. L'attacco con forza bruta è ancora più pericoloso quando si avvale dei dizionari, cioè elenchi di password di uso comune. Altra cosa da evitare nelle password è che siano riconducibili all'utente, perché in questo caso, potrebbe essere indovinata dall'umano, prima che dalla macchina, ed è comunque più vulnerabile agli attacchi di forza bruta che utilizzano come dizionario i dati conosciuti dell'utente.

Altro elemento importante, nel caso, ormai molto frequente, in cui si disponga di accessi a diversi sistemi (soprattutto portali Internet), è quello di non usare la stessa password per servizi diversi. In caso di violazione di un sistema, anche non per nostra colpa, i malintenzionati avrebbero a disposizione una password da provare a tappeto su migliaia di servizi Internet, con il rischio di poter accedere anche ad altri portali non direttamente violati.

Infine, è consigliabile cambiare il prima possibile le password assegnate da terzi e quelle di default di tutti i dispositivi: computer, i firewall, dispositivi di rete, NAS, stampanti, inclusi anche quelli meno "sospettabili", come condizionatori, macchinari industriali, ecc. (benché questi ultimi non contengano, né trattino dati, potrebbero divenire veicoli di attacchi ad altri dispositivi).

11.1.5 Idonea custodia delle password

La password è un elemento che ci identifica, come una carta d'identità nel modo digitale. Ciò che viene fatto sui sistemi, utilizzando il nostro nome utente e password, viene, almeno in prima battuta, ricondotto a noi. Sarà poi nostro onere dimostrare che le credenziali ci sono state sottratte: per questo motivo è importantissimo conservarle con estrema cautela. In particolare, occorre evitare di conservare la password su supporti cartacei o elettronici in luoghi dove potrebbe essere facilmente trovata. Possibilmente sarebbe opportuno non scriverla affatto, ma, normalmente, ci si trova ad aver a che fare con decine, se non centinaia, di password ed è umanamente impossibile

ricordarle tutte. Ci vengono in aiuto i *password manager*, software che permettono di mantenere un archivio cifrato di tutte le nostre password. A questo punto basta ricordare la password di accesso al password manager per poter accedere a tutte le credenziali di autenticazione.

Occorre, infine, sottolineare che è buona norma modificare le password con una certa frequenza (tipicamente qualche mese), anche nel caso in cui si sia ragionevolmente sicuri del fatto che nessuno ne sia venuto a conoscenza.

11.1.6 Gestione delle violazioni della password

Nel caso in cui si venisse a conoscenza del fatto che la nostra password è stata violata, ci si troverebbe di fronte ad un episodio di *data breach*, che dovrà essere gestito secondo vigente normativa e come descritto nel capitolo 2. A parte questo, le misure da prendere immediatamente sono diverse. Innanzitutto, la password deve essere sostituita ovunque sia stata impostata. È necessario, poi, sottoporre a scansioni anti-malware approfondite tutti i dispositivi accessibili con quella password, perché un malintenzionato potrebbe avervi inserito dei metodi di accesso fraudolenti (le cosiddette back-door). Occorre poi cercare le tracce di utilizzo della password (es. log degli accessi), per cercare di individuare eventuali attività malevole. Infine, occorre prestare attenzione alle attività possibili, compatibilmente con i poteri attribuiti a quella password. Per esempio, la password di un amministratore di sistema potrebbe aver permesso di creare un nuovo utente, rendendo vana la contromisura di sostituzione della password.

11.1.7 Segretezza della password

La password deve essere strettamente personale, e non deve essere comunicata a terzi. Se si rende necessario l'accesso al nostro sistema, in nostra assenza, è bene che sia stato previsto, in precedenza, un altro utente di accesso diverso dal nostro. Anche le tecniche di cifratura dei sistemi operativi, in genere, prevedono la possibilità di decifratura da parte di più utenti preimpostati nel sistema.

È molto importante anche fare attenzione a non comunicare accidentalmente elementi che possano far risalire alla password o, comunque, aiutare nella sua individuazione. Alcuni malintenzionati usano tecniche di cosiddetto *social engineering*, in cui vengono effettuate telefonate false, con l'intento di raccogliere elementi utili per la violazione dei sistemi informatici.

11.1.8 Idoneo smaltimento e consegna in assistenza dei dispositivi elettronici

Quando si smaltiscono dispositivi elettronici, o, comunque, nel caso in cui gli stessi debbano essere inviati in assistenza, occorre prestare attenzione al fatto che i dati non vengano trasferiti con il dispositivo. Nel caso dello smaltimento, può essere opportuno distruggere meccanicamente tutti i supporti digitali (tipicamente l'hard disk), oppure cancellarli mediante opportuni software di formattazione approfondita. Occorre evidenziare che, per esempio, la semplice rimozione della partizione di un hard disk, non è un metodo sicuro, in quanto facilmente reversibile.

Se viceversa, si sta inviando il dispositivo in assistenza, ove possibile, sarebbe opportuno rimuovere e trattenere i supporti digitali. Un'altra possibilità è quella di creare un utente limitato, in grado di accedere al sistema operativo (se l'accesso è necessario per le attività di assistenza), ma non di decifrare il disco dati (che dovrà, ovviamente, essere cifrato).

11.1.9 Idonee misure di conservazione e smaltimento della carta

Benché non si tratti di un supporto digitale, la carta, contiene molto spesso dati digitali stampati attraverso una stampante. La prima buona prassi sarebbe quella di evitare di stampare, se non è assolutamente necessario. Ove strettamente necessario, i documenti stampati devono essere conservati con estrema cura, e non lasciati incustoditi, se non sottochiave. Importante anche evitare di stampare e lasciare i fogli nella vaschetta della stampante per più tempo dello stretto necessario, soprattutto se, come spesso accade negli studi professionali, la stampante si trova in un'area aperta al pubblico (es. sala d'attesa).

Quando il documento dovrà essere smaltito, se contiene dati personali, dovrà essere opportunamente distrutto, in modo che i dati siano illeggibili e non ricostruibili. Sarebbe opportuno utilizzare un distruggi-documenti certificato. Particolare attenzione va posta nella prassi, comune in molti uffici, di "riciclare" il lato posteriore delle vecchie stampe. Nel caso in cui la stampa contenga dei dati personali, è opportuno che il "riciclo" avvenga ad opera di chi aveva eseguito la stampa originale, o, comunque, di chi ha titolo per accedere ai dati originali.

11.1.10 Idoneo comportamento durante la navigazione e l'utilizzo della posta elettronica

Come già detto in precedenza, la maggior parte delle violazioni ai dati dell'Ente, parte da programmi che vengono aperti come allegati di posta elettronica, o scaricati durante la navigazione. Per questo è molto importante prestare la massima attenzione nell'utilizzo di questi strumenti. È importante non fare mai cieco affidamento negli antivirus, antispam, firewall, ecc., perché questi sistemi, per quanto affidabili, non sono infallibili. Prima di aprire l'allegato in un messaggio di posta elettronica, è bene analizzare attentamente il messaggio. Il fatto di conoscere il mittente non è una garanzia, in quanto è estremamente semplice inviare messaggi di posta elettronica a nome di altri, e tutti i malware sfruttano estensivamente questa caratteristica. Attraverso sofisticati algoritmi che incrociano i dati di rubriche sottratte da computer compromessi, molti malware scelgono mittente e destinatario, garantendo un'elevata probabilità che questi si conoscano. Questo induce il destinatario a "fidarsi" del messaggio. Se ci sono dubbi sul contenuto del messaggio o anche solo se non si aspettava alcun allegato, è sempre bene verificare prima con il mittente se il messaggio è legittimo.

Un discorso analogo vale per i collegamenti presenti nei messaggi. In questo caso, oltre alla possibilità di scaricare virus, il rischio è anche quello della frode informatica denominata phishing. Si riceve un messaggio, per esempio dalla propria banca, in cui si viene invitati a verificare qualcosa, cliccando sul link. Se si clicca sul link, si viene indirizzati ad un sito malevolo che presenta una schermata simile a quella della banca, in cui vengono richieste le credenziali.

In generale potremmo accorgercene dall'indirizzo mostrato nella barra del browser (che può anche essere molto simile ma non uguale), o dal fatto che la connessione, in genere, non è sicura (non c'è il lucchetto o la barra verde), ma spesso non ci si fa caso. Nei casi più sofisticati, quelle stesse credenziali vengono addirittura passate al vero sito della banca, che ci fa entrare nel nostro conto. In questo modo non ci accorgiamo di nulla, ma il sito malevolo ha già rubato le nostre credenziali che, qualcuno, potrà utilizzare, successivamente, in modo indebito. Sarebbe sempre buona norma non fare click sui collegamenti nei messaggi di posta elettronica, ma entrare nei portali digitando direttamente l'indirizzo nel browser (o prendendolo dai preferiti).

In linea generale, è comunque bene evitare di accedere a siti non noti e di dubbia reputazione. Per esempio, le categorie di siti in cui più facilmente si possono scaricare malware, sono quelle relative al cosiddetto file sharing, ossia lo scambio di file multimediali in violazione del diritto d'autore.

11.1.11 Formazione del personale

L'informazione, sensibilizzazione e formazione del personale è sicuramente da annoverare nelle misure di prevenzione più efficaci per evitare che comportamenti superficiali o negligenti del personale interno all'organizzazione possano minacciare la sicurezza delle informazioni e, quindi, dei dati personali. Il Regolamento impone infatti che tutte le persone che trattano dati personali sotto il controllo del titolare del trattamento debbano essere istruite per farlo.

11.1.12 Procedure ed istruzioni per il personale

Unitamente alla formazione del personale è opportuno stabilire un sistema di disposizioni interne (procedure, istruzioni, ecc.) che da un lato permetta al personale di ricordare quali sono le linee di comportamento per un corretto trattamento dei dati personali e le conseguenze in caso di inosservanza delle stesse, dall'altro tuteli la Direzione dell'Ente o dello Studio rispetto ad eventuali azioni illecite eseguite dai dipendenti e dai collaboratori.

11.1.12 Impegni ed istruzioni per i fornitori

Un sistema di contratti con fornitori comprendenti, unitamente alla designazione dei responsabili esterni al trattamento se del caso, regole stabilite contrattualmente sul comportamento da osservare, modalità operative da attuare, impegni alla riservatezza, ecc. favorisce il rispetto delle regole e delle procedure stabilite e consente al titolare di mantenere maggior controllo sulle attività esternalizzate (es. elaborazione buste paga, tenuta della contabilità, outsourcing informatico, ecc.) e sulle attività svolte dai fornitori presso i locali dell'Ente (es. manutenzione hardware e software, consulenti, ecc.)

Oltre a predisporre contratti "robusti" con i fornitori è importante designare formalmente il personale dell'organizzazione che deve accedere ai dati e svolgere attività su di essi.

Infine, la nomina degli Amministratori di Sistema, dove esistono persone che in realtà svolgono questo ruolo, responsabilizza maggiormente queste figure e garantisce maggior tutela al titolare del trattamento.

11.2 Misure di sicurezza tecniche

11.2.1 Pseudonimizzazione dei dati

L'articolo 4 del Regolamento definisce la *pseudonimizzazione* come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

La pseudonimizzazione consiste nella pratica nel:

- *dividere* la componente identificativa del dato personale dalla sua componente sensibile ed attribuire all'interessato uno pseudonimo, che preso da solo non contribuisca ad identificare l'interessato,
- *attribuire* alle informazioni sensibili lo pseudonimo dell'interessato,
- *conservare* separatamente i dati identificativi dai dati sensibili.

Un attaccante recupera il dato personale completo solo se riesce ad accedere ad entrambi gli archivi dove sono conservati i dati identificativi e quelli sensibili.

Questa tecnica viene spesso utilizzata anche nei sistemi informatici: è buona norma prediligere software o servizi che adottano la pseudonimizzazione dei dati personali.

11.2.2 Cifratura dei dati

La cifratura è una tecnica che trasforma un dato in modo tale da renderlo illeggibile a meno della conoscenza di un segreto, di solito una password. Se un attaccante accede al dato senza conoscere il segreto, non è in grado né di leggerlo né tanto meno di ricondurlo all'interessato. La cifratura trova impiego in vari contesti, tra cui quelli in seguito descritti:

- Software e servizi con cifratura dei dati. Alcuni software in commercio, soprattutto quelli candidati al trattamento di dati la cui riservatezza rappresenta un fattore critico, conservano le informazioni in archivi cifrati, accessibile solo previo inserimento della password corretta. Nella scelta dei software da installare sui PC o servizi in *cloud* destinati al trattamento di dati personali è buona pratica prediligere quelli che implementano la cifratura degli archivi, soprattutto se vengono trattati dati appartenenti a particolari categorie e dati relativi a condanne penali e reati. La presenza di una password di accesso al software o al servizio non è garanzia della cifratura dei dati, consultare il manuale o chiedere informazioni specifiche al produttore per verificare l'effettiva presenza della funzionalità.

- Cifratura del sistema operativo. La maggior parte dei sistemi operativi moderni, dispone di tecniche di cifratura integrate. In generale, però, è necessario abilitarle. Può sembrare normale pensare che, la mancata conoscenza della password di accesso, prevenga dall'accesso al dispositivo. In generale, però, la password regola solo l'accesso al sistema operativo. Un malintenzionato che venga in possesso del dispositivo, potrebbe smontare l'hard disk (o altra memoria di massa), ed accedervi per mezzo di un altro dispositivo, recuperando tutti i dati, anche senza conoscere (o scoprire) la password. La cifratura del disco, scongiura questa possibilità, perché i dati in esso contenuti, saranno cifrati, qualunque sia il dispositivo a cui venga collegato. Molti moderni dispositivi (in particolare quelli mobili), dispongono di un componente hardware detto TPM (Trusted Protection Module): questo dispositivo contiene una chiave che è unica al mondo e che, combinata con la password dell'utente, genera una chiave di cifratura robusta. In questo modo, i dati sono accessibili solo su quello specifico dispositivo, e solo conoscendo la password dell'utente.
- Cifratura dei dispositivi rimovibili. La cifratura è particolarmente importante, soprattutto per i dispositivi rimovibili, in quanto tendono ad essere sempre più piccoli e sono facilmente distaccabili dal dispositivo a cui sono collegati. Un malintenzionato potrebbe sottrarre un dispositivo rimovibile in pochi secondi e portarlo con sé senza essere visto. I dispositivi rimovibili possono essere cifrati con le medesime metodologie utilizzate per cifrare il disco del sistema operativo. È possibile decidere di utilizzare il TPM, nel qual caso, il dispositivo rimovibile sarà utilizzabile solo sul PC su cui è stato cifrato, oppure limitarsi alla password, per esempio perché il dispositivo rimovibile deve essere condiviso fra più PC.

11.2.3 Software antivirus e anti-malware

I virus informatici, e similari (malware, spyware, trojan, ecc.), sono programmi per computer, espressamente sviluppati per arrecare danno ai contenuti del computer che ne viene infettato.

Inizialmente venivano sviluppati con finalità esclusivamente distruttive; oggi, si assiste sempre più, al proliferare di virus studiati per portare guadagni allo sviluppatore, tipicamente mediante la richiesta di un riscatto per "sbloccare" i dati (ramsonware). La diffusione di virus informatici è un reato penale in quasi tutti i paesi del mondo (in Italia art. 615 quinquies del Codice Penale, cui si aggiunge l'art. 640 ter c.p., se accompagnata da frode informatica), ma la percentuale di criminali assicurati alla giustizia è bassissima. Ad oggi, il principale veicolo di diffusione di virus ed altri malware informatici è la posta elettronica. Il virus può essere allegato al messaggio di posta elettronica, o, molto più spesso, essere presente in un collegamento che il messaggio stesso induce a cliccare. Ricevere o scaricare un virus, in sé, non comporta danni, fintanto che lo stesso non viene eseguito o installato. I programmi antivirus e anti-malware, si occupano di verificare la sicurezza di ogni singolo programma, prima che lo stesso venga eseguito, ed a bloccarlo (messa in quarantena), in caso di sospetto virus. I programmi antivirus analizzano i programmi, sulla base di numerosi criteri, di cui, il principale, è la presenza di opportuni pezzi di codice in una lista di virus noti. Per questo motivo, è opportuno, non solo installare un programma antivirus, di primaria diffusione, su ogni PC e server, ma assicurarsi anche che lo stesso venga aggiornato con cadenza almeno giornaliera (l'aggiornamento avviene automaticamente, ma a volte potrebbe non funzionare).

11.2.4 Software firewall/antintrusione

In uno scenario in cui qualsiasi PC o Server è dotato di una connessione a Internet, risulta possibile, per un malintenzionato, accedere ai dati digitali, all'insaputa del titolare. Per l'utente comune di un PC, è estremamente difficile accorgersi dell'intrusione, perché non viene presentato nulla a schermo e le tracce lasciate sono poche e nascoste. Anche l'intrusione in sistemi informatici è un reato penale (in Italia art. 615 ter del Codice Penale), ma, anche in questo caso, è difficile risalire al responsabile, che, normalmente, maschera la propria identità, facendo "ponte" in paesi extra UE, dove la richiesta di rogatorie è molto difficile.

Come nel caso dei virus, esistono software in grado di proteggere un dispositivo informatico dalle intrusioni, chiamati comunemente firewall. Molto spesso questi strumenti sono accessori al software antivirus (di serie o acquistabili in opzione), e sono, in parte, integrati nei sistemi operativi moderni (personal firewall). Anche questo

tipo di software necessita di aggiornamenti frequenti, perché le logiche di attacco cambiano e gli strumenti di difesa si adeguano di conseguenza.

11.2.5 Aggiornamenti di sicurezza del software

Come già visto per i software antivirus ed antintrusione, qualsiasi tipo di software necessita di aggiornamenti periodici, che, l'Ente produttrice, mette a disposizione per sopperire ad eventuali vulnerabilità individuate dopo il rilascio del software stesso. Praticamente nessun software informatico è esente da vulnerabilità di sicurezza, ed un malintenzionato potrebbe sfruttarle per danneggiare o sottrarre dati. Quando i produttori di software rilasciano un aggiornamento di sicurezza, in pratica, rendono disponibile a chiunque dettagli sulla vulnerabilità sanata, utili anche per sfruttarla malevolmente. Per questo motivo è molto importante applicare il prima possibile gli aggiornamenti di sicurezza ai sistemi operativi, ed a qualunque altro software presente sul dispositivo. Quasi tutti i dispositivi permettono di configurare gli aggiornamenti automatici, per garantire sempre la massima protezione. Una nota molto importante è relativa alla durata del supporto che, il produttore del software, garantisce. I programmi più vecchi, spesso, sono fuori dal periodo di supporto, ed eventuali problemi di sicurezza non vengono più risolti. È molto importante verificare che tutti i sistemi operativi ed i programmi utilizzati, godano ancora del supporto e degli aggiornamenti di sicurezza. In caso contrario, è consigliabile sostituire, il prima possibile, il software con uno più recente.

11.2.6 Idonea gestione degli accessi WiFi

Il WiFi costituisce una infrastruttura di rete, con i medesimi privilegi di accesso di una rete cablata, ma con elementi di sicurezza molto inferiori. Per ottenere l'accesso alla rete cablata, è necessario ottenere l'accesso fisico all'armadio di commutazione o ad una presa a muro attiva, mediante un dispositivo dotato di rete cablata. Questa attività, in genere, è difficilmente occultabile. Le reti WiFi, di contro sono, spessissimo, accessibili anche dalla strada, e con dispositivi anche molto piccoli (smartphone). La presenza di una password di accesso al WiFi, benché aiuti, è un falso elemento di sicurezza, perché in caso la rete WIFI sia configurata con protocolli di comunicazione deboli, con le tecniche che abbiamo visto in precedenza (che nel caso del WiFi tengono conto anche del traffico effettuato da dispositivi "leciti", riducendo enormemente i tempi), la password può essere individuata in tempi ragionevoli. Inoltre, la password del WiFi non è personale e, tendenzialmente, non viene mai cambiata, diventando, ben presto, nota a molte persone. Sarebbe opportuno che le reti WiFi non fossero connesse alla rete dell'Ente, ma, solo se necessario, vi accedessero attraverso un Firewall (un po' come se l'accesso avvenisse da Internet).

11.2.7 Idonea configurazione dell'accesso a internet

La tendenza odierna è quella di connettere qualsiasi dispositivo ad Internet, a prescindere dal suo utilizzo. In realtà esistono dispositivi (tipicamente server, ma non solo), che non necessitano di essere connessi a Internet. Sarebbe buona prassi individuare le necessità di connessione ad Internet di ciascun dispositivo, ed effettuare (o non effettuare) la connessione dello stesso, con il minimo insieme di privilegi necessari. Ad esempio, per un server, spesso non è necessaria la connessione ad Internet, fatta eccezione per le funzioni a cui è preposto. Per un server di posta elettronica, ad esempio, si deve abilitare la ricezione e l'invio della posta, la ricezione degli aggiornamenti dei software e degli antivirus, ma è sconsigliato consentire la navigazione del Web. Queste limitazioni, generalmente, possono essere imposte mediante gli strumenti di configurazione del sistema operativo.

11.2.8 Firewall/router

In questo caso, però, si tratta di un dispositivo di rete fisico, che, a differenza del software, non si prepone di proteggere un unico computer, ma tutta la rete dell'Ente. È importante dotare la propria rete di un Firewall di primaria diffusione, e di configurarlo opportunamente per minimizzare i punti di esposizione a Internet (le cosiddette porte aperte). In uno scenario ideale, tutte le porte, da Internet verso la rete dell'Ente, dovrebbero essere chiuse. Spesso, però, è necessario aprirne alcune, per permettere il funzionamento di servizi, come server di posta o siti Internet. È molto importante che la configurazione del Firewall venga fatta tenendo conto delle più recenti linee guida di sicurezza, e che la stessa venga revisionata frequentemente, per rispondere ad eventuali vulnerabilità scoperte in fasi successive.

Il *firmware* del Firewall (cioè il suo sistema operativo) deve essere mantenuto aggiornato, secondo le direttive del produttore. Anche in questo caso, è importante che il produttore garantisca il supporto e gli aggiornamenti di sicurezza. Nel caso di Firewall obsoleti, è consigliabile, sostituirli, il prima possibile, con dispositivi più moderni. I più comuni Firewall, oltre a proteggere dalle intrusioni (dall'esterno verso l'interno), proteggono anche la navigazione dei dispositivi connessi in rete dell'Ente (dall'interno verso l'esterno), bloccando, per esempio, siti malevoli, prima che possano compromettere la sicurezza informatica. I più moderni Firewall sono dotati di sistemi antivirus, antimalware, antispam, ecc. Inoltre, dispongono di dispositivi attivi di protezione dalle intrusioni, cioè non si limitano a chiudere le porte, ma analizzano il traffico digitale, attraverso le porte aperte, alla ricerca di comportamenti malevoli. Infine, dispongono di sistemi di filtro e protezione della navigazione, per bloccare l'accesso a siti malevoli, o appartenenti a determinate categorie potenzialmente pericolose o illegali. Tutti questi servizi attivi devono essere aggiornati molto frequentemente (tipicamente giornalmente) ed in modo automatico. I produttori di Firewall rendono disponibili contratti di aggiornamento di questi servizi, che è opportuno sottoscrivere.

È opportuno sottolineare nel caso si colleghino dispositivi portatili a reti diverse da quella dell'Ente, il firewall di rete non protegge in questo caso i suddetti dispositivi, che andranno dunque dotati di un software Firewall.

11.2.9 Backup e disaster recovery

Virus, attacchi informatici, ed altri metodi di sabotaggio, non sono gli unici rischi per l'integrità e la disponibilità dei dati. Anche eventi come guasti dei sistemi, catastrofi naturali, o semplicemente, errori umani, commessi in buona fede, possono comportare la modifica non desiderata o addirittura la perdita di dati. Benché i dispositivi critici (server) siano quasi sempre dotati di sistemi di ridondanza dei dati, è comunque necessario eseguire periodicamente delle copie di salvaguardia dei dati stessi (backup). I backup devono essere eseguiti con una frequenza che dipende sia dall'importanza dei dati, che, soprattutto, dalla loro dinamicità. Per esempio, per dati che vengono aggiornati con cadenza mensile, è possibile ipotizzare un backup mensile (coincidente con il giorno di modifica dei dati), mentre per i dati "correnti", cioè sottoposti ad aggiornamenti continui, è bene pensare ad un backup con cadenza almeno giornaliera. Molto importante anche il tempo di conservazione dei backup. Non è raro che la cancellazione accidentale di una porzione di dati venga scoperta a settimane di distanza dall'evento. In questi casi, un backup recente non aiuterebbe a recuperarli. In generale, è buona norma poter "tornare indietro nel tempo" di almeno 1 mese, possibilmente anche di più (compatibilmente con le capacità dei supporti di archiviazione dei backup). Molto importante è anche eseguire, periodicamente, delle prove di ripristino (restore), cioè simulazioni di recupero dei dati come se fossero stati persi. Questo evita di trovarsi, all'occorrenza, con copie di backup corrotte o incomplete. È importante anche garantire che eventuali eventi disastrosi, come una calamità naturale, che possano compromettere i dispositivi "correnti", non vadano a compromettere anche i supporti di backup. Si possono adottare diverse strategie, dall'asportazione dei supporti di backup (cassette da portare a casa), all'esecuzione delle copie in posizioni fisicamente distanti dagli originali, inclusi i backup in Cloud. Occorre, però, tenere conto del fatto che la "delocalizzazione" delle copie di backup, rispetto all'ambiente fisicamente protetto in cui si trovano, normalmente, i server, può aumentare il rischio di furti. Per questo è bene adottare misure di sicurezza maggiori sui supporti di backup. La maggior parte dei software di backup permette di eseguire la cifratura delle copie. Questa misura genera delle copie illeggibili, a meno di non disporre della chiave di decifratura, generalmente molto complessa e difficilmente identificabile (e, soprattutto, non salvata sui supporti di backup). La cifratura dei dati, anche a norma del Regolamento, rappresenta una forma di protezione idonea alla conservazione dei dati anche in ambienti non sicuri.

Guasti, calamità ed errori, oltre a comportare il rischio di perdita di dati, mitigato, come abbiamo visto, dalla corretta gestione dei backup, comportano anche un rischio di perdita (temporanea) di disponibilità dei dati. Se, per effettuare il restore (e/o per riparare il guasto), occorre molto tempo, per tutto questo tempo, il dato non è disponibile. Per mitigare questo rischio, entrano in gioco le tecniche di disaster recovery. In pratica, le tecniche di *disaster recovery*, effettuano delle copie, simili ai backup, ma tali da poter rendere disponibili i dati (ed i software

di trattamento) in tempi molto brevi, anche in caso di indisponibilità del dispositivo originale. Molto spesso queste tecniche si basano sul principio di rendere disponibile, in Cloud o altro ambiente idoneo, una copia gemella del dispositivo che si è guastato, con tutto il suo contenuto in termini di software e dati. il tutto avviene in termini di decine di minuti, anziché di giorni.

11.2.10 Utilizzo del Cloud

Collocare dati in *Cloud*, in linea di principio, non pone rischi di sicurezza. I server dei primari fornitori Cloud, sono, tendenzialmente, molto più sicuri dei nostri server dell'Ente, perché vi sono decine di persone che, per lavoro, si occupano solo di sicurezza informatica. Il punto è sempre quello di utilizzare un fornitore affidabile, ed un servizio conforme al Regolamento. Tutti i principali fornitori Cloud offrono oggi questo genere di servizi. Un aspetto molto importante della conformità è quello di mantenere i dati all'interno dell'Unione Europea oppure in Paesi per i quali esiste una decisione di adeguatezza del Comitato o altre forme di garanzia riconosciute dal Regolamento (Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali). Naturalmente sono da considerare anche gli aspetti di sicurezza, backup, disaster recovery, cifratura dei dati, ecc. La prima cosa che sarebbe opportuno ottenere dal fornitore è la dichiarazione di rispondenza al Regolamento. Molto spesso è possibile scaricarla dal sito stesso, a volte "tagliata" sui servizi che stiamo utilizzando, e corredata di descrizione tecnica dei metodi utilizzati per garantire la conformità. È bene sottolineare che tutto ciò è presente nei servizi di tipo "business" (a pagamento), ma, in genere, non in quelli di tipo "consumer" (solitamente gratuiti). Per questi ultimi, la conformità al Regolamento non viene garantita e, pertanto, sarebbe opportuno non utilizzarli per archiviare dati personali.

Quasi tutti i servizi di memorizzazione su Cloud prevedono la cifratura dei dati all'origine, ovvero i dati vengono cifrati prima di partire dal nostro PC ed essere trasferiti al Cloud, e decifrati nel nostro PC dopo essere stati scaricati dal Cloud. Questa funzione garantisce la massima protezione dei dati ed andrebbe sempre attivata, in particolar modo, se il servizio Cloud viene utilizzato anche da dispositivi mobili, su reti WiFi che potrebbero non essere sicure. Se la cifratura/decifratura avviene sul dispositivo, è, ad oggi, impossibile intercettare i dati.

11.2.11 Profilazione utenti

La profilazione degli account degli utenti nei sistemi (file server, sistemi gestionali, applicativi web, ecc.) permette di limitare l'accesso ai dati personali solo al personale che necessita di lavorare su quei dati. Purtroppo non sempre i sistemi gestionali permettono una segmentazione degli accessi tale per cui effettivamente solo i dati necessari sono consultabili da ogni utente, tuttavia è in corso una forte evoluzione tecnologica a supporto della protezione dei dati personali.

La configurazione dei profili utente, anche e soprattutto in ambiente Windows (che è quello che solitamente rappresenta la prima porta di accesso ai documenti ed ai dati) non va solo definita correttamente "una tantum", va anche aggiornata a fronte di variazioni che si verificano nell'organizzazione (assunzioni e dimissioni, cambiamenti di ruolo o mansione, interruzione dei rapporti di collaborazione).

12 Policy per la gestione del "Data Breach"

12.1 Definizioni ed identificazione delle violazioni

L'art. 33 (Notifica di una violazione dei dati personali all'autorità di controllo) del Regolamento Europeo 679/2016 (GDPR) impone al titolare del trattamento di notificare all'autorità di controllo, ed in alcuni casi anche agli interessati, la violazione di dati personali (*data breach*) entro settantadue ore dal momento in cui ne viene a conoscenza.

Già in precedenza sussisteva l'obbligo di notifica delle violazioni di dati personali, per particolari categorie di titolari o per particolari categorie di trattamenti, ma la novità del GDPR è l'estensione dell'obbligo a tutti i titolari.

Il legislatore europeo richiede, quindi, che tutte le realtà toccate dal Regolamento siano in grado di rispettare i requisiti di trasparenza, evidenza e responsabilità. A tal proposito, si ricorda che l'art. 24 punto 1 del GDPR richiede al titolare di "mettere in atto misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR".

12.1.1 Notifica/Comunicazione

L'obbligo di notifica all'Autorità di Controllo scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche; qualora il rischio sia elevato, oltre alla notifica, il titolare è tenuto a darne comunicazione anche all'interessato. Il termine per adempiere alla notifica è brevissimo, settantadue ore dal momento in cui il titolare ne viene a conoscenza, mentre l'eventuale comunicazione agli interessati deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato; il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati) e la imposizione di sanzioni amministrative secondo l'art. 83 GDPR , il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Occorre in ogni caso tenere conto del fatto che la mancata notifica e/o comunicazione, può rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali, quali ad esempio, carenze od inadeguatezza di misure di sicurezza; in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.

Il rispetto degli obblighi di notifica (art. 33) e di comunicazione (art. 34), in realtà già mediamente complesse (in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati), richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda una procedura per la gestione degli incidenti e la continuità operativa.

12.1.2 Violazione di dati

Per "Violazione di dati" si intende la violazione 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 p.12 GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

Si possono distinguere tre tipi di violazioni:

- Violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
- Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
- Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

12.1.3 Identificazione dell'incidente di sicurezza

Il considerando 85 offre utili elementi per determinare i rischi che possono determinare l'obbligo di notifica. In particolare, occorre valutare la possibilità che la violazione possa causare danni fisici, materiali o immateriali alle persone fisiche. La disposizione a titolo d'esempio elenca:

f) perdita del controllo dei dati personali che li riguardano;

g) limitazione dei loro diritti; discriminazione;

h) furto o usurpazione di identità;

i) perdite finanziarie;

j) decifratura non autorizzata della pseudonimizzazione;

k) pregiudizio alla reputazione;

l) perdita di riservatezza dei dati personali protetti da segreto professionale;

m) o qualsiasi altro danno economico o sociale significativo per la persona interessata.

L'art. 33 p.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine

di consentire all'autorità di controllo di verificare il rispetto della norma. Ne discende che le generali

attività di rilevazione dell'incidente, come le successive di trattamento, devono essere:

j) documentate;

k) adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi);

l) tracciabili;

m) replicabili.

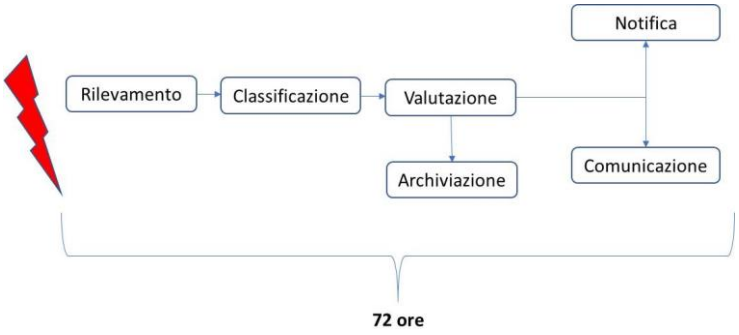
Di quanto sopra il titolare deve essere in grado di fornire evidenza nelle sedi competenti.

È importante, altresì, che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica; peraltro è rilevante considerare che scoprire l'incidente non è sufficiente, il titolare deve essere in grado di valutare la portata di questo in termini di impatto rispetto ai dati personali ed ai diritti e la libertà degli interessati.

La rapida identificazione dell'incidente e la tempestività della adozione di contromisure possono consentire di limitare i danni derivanti da una violazione a carico degli interessati.

Nella definizione del processo di gestione del *data breach* diventa importante tenere conto di situazioni in cui il Titolare abbia affidato servizi a Responsabili del trattamento; preliminarmente, deve essere accertata la capacità del fornitore nel gestire tempestivamente e adeguatamente un incidente di sicurezza (art. 28 p.1 GDPR) e, quindi, è necessario prevedere idonee clausole contrattuali (art. 28 p.3 GDPR) che regolino il rapporto di fornitura in modo da garantire il rispetto del GDPR.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.



L'art. 34 del GDPR stabilisce che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare deve comunicare la violazione all'interessato senza ingiustificato ritardo. Il considerando 86 del GDPR chiarisce che l'obbligo di comunicazione risponde allo scopo di consentire all'interessato, qualora sussista una violazione che presenta rischi elevati, di prendere le precauzioni necessarie.

La Notifica e la Comunicazione hanno un contenuto pressoché identico.

Notifica - Art. 33 p.3 GDPR

e) 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.

f) Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o, in sua assenza, i dati del Delegato Privacy

g) Descrivere le probabili conseguenze della violazione dei dati personali.

h) Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Comunicazione - Art. 34 p.2 GDPR

- Descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali.
- Comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o, in sua assenza, i dati del Delegato Privacy presso cui ottenere più informazioni.
- Descrivere le probabili conseguenze della violazione dei dati personali.

- Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

La comunicazione dovrebbe essere data direttamente e personalmente agli interessati coinvolti dalla violazione, a meno che ciò comporti sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con la medesima efficacia.

12.1.4 Valutazione del livello di criticità della Violazione

Il considerando 76 del GDPR chiarisce che la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

L'EDPB suggerisce ulteriori criteri per permettere una valutazione più accurata.

k) Tipo di violazione;

l) Natura, sensibilità e volume dei dati personali;

m) Facilità di riconoscimento degli interessati;

n) Serietà delle conseguenze per le persone fisiche;

o) Caratteristiche specifiche delle persone fisiche;

p) Quantità di persone fisiche coinvolte;

q) Caratteristiche specifiche del titolare.

La valutazione dei rischi non sempre è semplice; a tal proposito il WP29 raccomanda al titolare, in caso di dubbio, di scegliere la strada di maggior tutela procedendo alla notifica.

12.1.5 Procedura di identificazione e gestione degli incidenti

La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.

La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).

Infine, è possibile mostrare la stessa documentazione delle violazioni, che la norma prescrive di conservare, (anche per quelle che non determinano obbligo di notifica), solo se è stato strutturato un sistema di gestione degli incidenti.

12.2 Processo di gestione degli incidenti di sicurezza

Di seguito si riporta una proposta di flusso di processo relativo alla gestione degli incidenti nonché la procedura di gestione dei data breaches prevista dal Regolamento.

Il trattamento degli incidenti di sicurezza presuppone, a monte, l'esistenza di un sistema di sicurezza delle informazioni che offra tutti gli strumenti necessari.

1. La scoperta dell'incidente presuppone un sistema di monitoraggio che, a sua volta, presuppone l'organizzazione della sicurezza all'interno dell'Ente (definizione degli obiettivi, politiche, compiti e responsabilità, classificazione di dati e processi, individuazione e definizione dei rischi, individuazione dei rimedi).
2. La valutazione dell'incidente presuppone la definizione dei criteri di valutazione, la formazione del personale incaricato, la predisposizione di procedure.
3. La tempestività nella notifica può essere assicurata se preesiste un sistema di comunicazione interno adeguato e tutti coloro che operano per il titolare abbiano ricevuto adeguata formazione.
4. La stessa comunicazione può essere fatta solo se sono disponibili le informazioni necessarie, aspetto possibile solo se precedentemente è stato strutturato un sistema di report dell'incidente, è stata fatta una ricognizione adeguata dell'organizzazione del titolare, sono state condotte le Valutazioni di impatto sui dati personali (DPIA).
5. Infine, è possibile mostrare la stessa documentazione delle violazioni, che la norma prescrive di conservare, (anche per quelle che non determinano obbligo di notifica), solo se è stato strutturato un sistema di gestione degli incidenti.

Una corretta gestione delle problematiche di *data breach* deve anche basarsi su una serie di presupposti organizzativi. In particolare:

1. Tutti gli attori coinvolti devono essere allineati su cosa sia un incidente di sicurezza.
2. Tutti gli attori devono essere allineati sulla classificazione e la casistica relativa agli incidenti di sicurezza.
3. Tutti gli attori devono essere allineati sul fatto che gli incidenti di sicurezza devono essere gestiti da un team con apposite competenze e che tale funzione opera sotto la responsabilità del rappresentante legale con il controllo della Direzione.
4. In qualunque punto del processo, laddove non ci sia risposta sollecita da parte di utenti e funzioni interne o del Responsabile del trattamento, sarà compito della Direzione attivare le necessarie escalation sul Titolare del Trattamento, identificato nel Legale Rappresentante della Ente, con il coinvolgimento del DPO.

Nel seguito è riportata una sintetica descrizione del processo suddiviso in fasi come indicato nello schema che segue.

- Rilevamento e Segnalazione
- Analisi e Classificazione

- Trattamento incidente
- Chiusura incidente
- Follow up e Reporting

12.2.1 Rilevamento e Segnalazione

La fase di rilevazione del processo di gestione degli incidenti ha la principale finalità di intercettare ed identificare tutti i possibili eventi che possano essere correlati ad un potenziale incidente.

La rilevazione e segnalazione può essere riconducibile, in particolare, a due principali fonti:

- Rilevazione Interna proveniente da personale dell'Ente (utenti autorizzati al trattamento). Il personale dell'Ente può identificare:
  - eventi di sicurezza sui sistemi o componenti di sistema gestiti internamente;
  - eventi di sicurezza relativi ai sistemi eventualmente gestiti da Responsabili del trattamento;
  - possibili eventi di sicurezza per altri servizi gestiti da altri fornitori.
- Rilevazione Esterna – Eventuali fornitori esterni, a prescindere che siano stati o meno nominati, l'interessato, Responsabili del trattamento che identificano eventi di sicurezza mediante rilevazione e/o segnalazione.

Segnalazioni di eventi di sicurezza possono sorgere all'interno dell'Ente, anche da parte di funzioni interne o di partner/fornitori esterni con i quali la stessa collabora.

Tutte le segnalazioni che pervengono sia da fonti interne all'Ente sia da eventuali fornitori esterni di cui l'Ente si avvale, vengono raccolte ed analizzate preliminarmente dalla Segreteria Generale al fine di effettuare una prima analisi e filtrare quelle ritenute non significative.

Le informazioni necessarie alla valutazione dell'incidente devono comprendere:

- gli asset impattati sia in numero che in tipologia;
- la criticità, la classificazione del processo di gestione del rischio, degli asset coinvolti;
- i processi, i servizi e i soggetti impattati dall'evento;
- eventuali danni prodotti dall'evento (es. malfunzionamenti, blocchi o degradi di servizi, corruzione di dati, fughe di informazioni, etc);
- in caso di attacco da Internet, sorgenti (es. indirizzi IP), estensione e modalità di attacco;
- altre segnalazioni/allarmi correlati all'evento in esame;
- modalità di propagazione/evoluzione dell'evento;
- altre informazioni ritenute utili.

Tutte le informazioni suddette hanno la finalità di consentire la classificazione dell'evento e di attivare tutte le misure di contrasto e contenimento necessarie.

Qualora la segnalazione sia riconducibile a un evento di sicurezza, la Segreteria Generale (o suo incaricato) invierà una e-mail all'indirizzo specifico xxx.

Nel caso di "evento di sicurezza", saranno coinvolte le funzioni "privacy" per la successiva classificazione di dettaglio. In tal caso tutte le funzioni delegate e i loro collaboratori, essendo informati della segnalazione dell'evento di sicurezza, potranno già intraprendere le azioni opportune per la gestione e la risoluzione dell'incidente.

12.2.2 Analisi e classificazione

L'analisi e la classificazione di dettaglio degli eventi di sicurezza ad opera dell'Amministratore di Sistema ha la principale finalità di avviare le necessarie attività volte a raccogliere le informazioni indispensabili per la corretta classificazione dell'evento di sicurezza. L'attività di classificazione tipizza l'evento in "falso positivo" o in caso di "incidente" effettivo lo categorizza in modo più granulare, sulla base della gravità (in incidente operativo, incidente di sicurezza informatica, incidente grave, crisi) guidando così le attività necessarie per il suo trattamento.

Sulla base delle informazioni fornite riguardanti l'entità dell'incidente sarà cura del Titolare del Trattamento provvedere alla valutazione d'impatto dell'incidente sul proprio contesto operativo e prendere una decisione in merito alla necessità di procedere alla "Notifica" e alla "Comunicazione".

12.2.3 Trattamento

La fase di trattamento del processo di gestione degli incidenti ha la principale finalità di attivare tutte le azioni necessarie a gestire l'evento segnalato.

Una volta ricevuta la segnalazione dell'evento, la fase di trattamento consiste nella presa in carico dell'incidente e nell'attuazione di tutte le misure di contenimento e riduzione degli impatti da porre in essere.

Nel caso di incidente di sicurezza dovrà essere mantenuto un opportuno aggiornamento mediante canali tempestivi (telefonicamente e/o via sms) tra i referenti interni all'Ente ai fini di consentire agli stessi visibilità costante sullo stato di avanzamento della gestione e risoluzione dell'incidente e di rispettare le tempistiche stringenti previste dal Regolamento.

Il Titolare del Trattamento procederà, nel rispetto dei tempi richiesti, ad attivare la notifica all'autorità di controllo competente. Analoga azione dovrà essere fatta nel caso in cui si evidenzi la necessità di comunicazione dell'incidente al / ai soggetti interessati.

12.2.4 Chiusura Incidente

Nel momento in cui l'evento viene risolto, il Titolare del Trattamento effettua la verifica di quanto risolto e procede all'aggiornamento del sistema di gestione degli incidenti.

Il sistema di gestione degli incidenti di sicurezza dovrà contenere tutte le informazioni raccolte anche per quelle segnalazioni che non hanno determinato un obbligo di notifica o di comunicazione.

12.2.5 Follow up e Reporting

La fase di Follow-up & Reporting ha la finalità di analizzare le cause che hanno determinato il verificarsi dell'incidente e di identificare gli interventi necessari affinché lo stesso non si ripeta.

Il Titolare del Trattamento, dietro suo incaricato, a tal fine predispone e protocolla la relazione tecnica di chiusura dell'intervento indicando le cause che hanno determinato l'evento/incidente, gli interventi e le eventuali contromisure adottate, nonché tutte le informazioni raccolte in fase di classificazione e analisi e, per quanto riguarda gli incidenti, le azioni di contrasto, contenimento e ripristino adottate, le vulnerabilità/minacce riscontrate, con indicazione della relativa gravità.

Gli eventi qualificati come *data breach* ai sensi dell'art. 33 vengono tracciati mediante annotazione su apposito Registro recante le seguenti voci:

- data e tipo di evento;
- numero di risorse informatiche coinvolte;
- numero di utenti/postazioni di lavoro potenzialmente impattati dalla indisponibilità del servizio informatico;
- risorse ICT /utenti esterni coinvolti;
- tipo di danno arrecato;
- enti/organizzazioni coinvolti nell'incidente;
- modalità di gestione dell'incidente.

Allegati

Allegato 1 – Policy per l'Utilizzo degli strumenti informatici dell'Ente

Allegato 2 – Violazione di dati personali – Modello di notifica al Garante