ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

L'importanza della formazione nella protezione dei dati personali

Un esempio di formazione per la filiale bancaria

Cesare De Santis

Roma 24/03/2023

Agenda

- Presentazione relatore
- L’importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Bibliografia & sitografia
- Q&A

Agenda

Presentazione relatore

- L’importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Bibliografia & sitografia
- Q&A

Presentazione relatore (1/2)

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa/Aeronautica) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl a socio unico, che opera principalmente sui temi della conformità normativa e della protezione dei dati personali. Tra i clienti di PRIMAe srl si annoverano associazioni bancarie, banche, finanziarie, rappresentanze italiane di compagnie di assicurazione europee, altre società di consulenza. Assicuriamo il servizio DPO ad alcune banche.

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM e certificazione UNI 11697:2017

Agenda

- Presentazione relatore
- L’importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- **L'importanza della formazione nella protezione dei dati personali**
- Un esempio di formazione per la filiale bancaria
- Q&A
- Bibliografia & sitografia

Gli obblighi derivanti dal GDPR e da altri provvedimenti

- «*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati* ***se non è istruito in tal senso dal titolare del trattamento****, salvo che lo richieda il diritto dell'Unione o degli Stati membri*» (Art. 29 GDPR)
- *«Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati* ***se non è istruito in tal senso dal titolare del trattamento****, salvo che lo richieda il diritto dell'Unione o degli Stati membri.»* (Art. 32 c.4 GDPR)
- *« … Resta parimenti ferma la necessità che, nell´individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi,* ***sia svolta un´attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni*** *(cfr. Allegato B al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9) …»* (punto 8 del provvedimento «Lavoro: le linee guida del Garante per posta elettronica e internet»)

Il ruolo del DPO

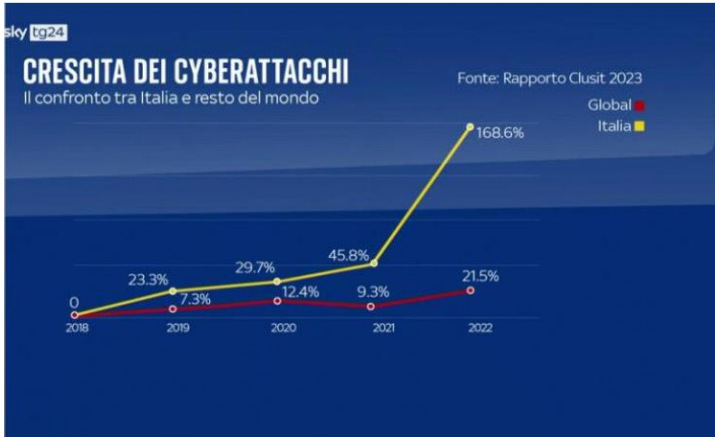
- Tra i compiti del DPO è riportato quello di « ***sorvegliare l'osservanza del presente regolamento***, *di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali,* ***compresi*** *l'attribuzione delle responsabilità,* ***la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo***» [art. 39 c.1 lettera b) del GDPR]
- Nel «Manuale RPD» pubblicato sul sito del Garante privacy tra i compiti di informazione e di sensibilizzazione interna attribuiti a questa figura è riportato che «*Le misure adottate dal RPD a tal fine includono l'elaborazione di note (o circolari) di informazione al personale,* ***l'organizzazione di sessioni interne di formazione sulla protezione dei dati*** *– finalizzate a sensibilizzare e migliorare la consapevolezza sulla protezione dei dati e i diritti dei soggetti interessati, cioè alla creazione di un "riflesso automatico" di protezione dei dati a tutti i livelli della vita sociale, in quanto semplici cittadini, lavoratori, team leader, dirigenti. In queste misure includiamo anche la creazione di un sito web interno di informazione e didattica sulla protezione dei dati e la redazione e l'invio di informative sulla privacy sui siti web e le pagine web del personale*

Relazione con la formazione sulla sicurezza

Il binomio sicurezza e formazione ha rivestito sempre grande importanza nella protezione dei dati personali sia nella normativa previgente(1) che in quella attuale (cfr. il già citato art. 32 c. 4 del GDPR).

Nelle aziende, in particolare nelle banche, considerando che:

- ✓ i rischi cyber sono aumentati esponenzialmente,



- ✓ il personale non formato costituisce punto debole nei presidi aziendali contro tali rischi;

negli ultimi anni sono stati intrapresi programmi di «*security awareness*» che comprendono:

- ✓ formazione del personale sulla sicurezza in generale e sulle cautele da adottare per minimizzare i rischi cyber;
- ✓ comunicazioni sistematiche di *alert* per segnalare eventi che possano costituire minacce per la sicurezza aziendale;
- ✓ predisposizione opuscoli informativi per dipendenti e clienti;
- ✓ test periodici (es. invio di finte email con contenuti potenzialmente pregiudizievoli) della capacità del personale di percepire e quindi contrastare i rischi.

(1) («*la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare*» era uno degli elementi che dovevano caratterizzare il Documento Programmatico sulla Sicurezza)

Agenda

- Presentazione relatore
- L’importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- L'importanza della formazione nella protezione dei dati personali
- **Un esempio di formazione per la filiale bancaria**
- Q&A
- Bibliografia & sitografia

La Filiale bancaria oggi

- Nonostante il fenomeno della c.d. «desertificazione» bancaria (secondo la FIRST/CISL il 40% dei Comuni è privo di sportelli e nel 2022 ne sono stati chiusi 554, oltre 2% in meno rispetto al 2021) la filiale bancaria continua ad avere grande importanza per le banche, soprattutto per le c.d. «banche del territorio» (1)
- La filiale, per questi istituti, è ancora il primo, e più importante, punto di contatto con la propria clientela
- La sua operatività deve essere quindi caratterizzata dalla massima conformità alle norme che incidono sull'attività bancaria, tra le quali si segnala, per importanza e gravità del quadro sanzionatorio, proprio la *data protection*
- La formazione del personale sulla *data protection* è un elemento indispensabile per raggiungere tale conformità

(1) «… *Con "Banca del territorio" intendo indicare quella tipologia di banca che si autocolloca fra i fattori locali avendoli come riferimento principale e mantenendovi le relazioni necessarie alla costruzione di un sistema territoriale di sviluppo economico e sociale, ovvero allo sviluppo di progetti, analisi economico-sociali e soluzioni condivise. La "Banca del territorio" è dunque parte integrante di quella rete economico-sociale e culturale che forma ciò che identifica il territorio e che costituisce il mercato di riferimento della Banca. Ciò la differenzia sostanzialmente dalle altre banche che pur operando nel territorio non lo considerano quello di riferimento*… « (da «La banca del territorio» di Paolo Romeo in www.aism.org)

Formazione per la filiale bancaria

La protezione dei dati personali in Filiale

Banca ....

Corso di aggiornamento

.....

Inquadramento normativo e definizioni (1/3)

RICHIAMI NORMATIVI E DEFINIZIONI (1/3)

Normativa di riferimento

- Regolamento UE 2016/679, conosciuto anche come «General Data Protection Regulation» (da cui l'acronimo «GDPR»)
- D.lgs. 196/2003, come modificato al D.lgs. 101/2018, conosciuto anche come «Codice privacy»

Inquadramento normativo e definizioni (2/3)

RICHIAMI NORMATIVI E DEFINIZIONI (2/3)

DEFINIZIONI UTILI

Dato personale: qualsiasi informazione riguardante una persona fisica[1] identificata o identificabile («interessato») → art. 4 c. 1 GDPR

Dati appartenenti a particolari categorie: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona → art. 9 GDPR

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 → art. 4 c. 2 GDPR

(1) In alcuni provvedimenti del Garante privacy le ditte individuali sono considerate persone fisiche (vedi ad esempio "Ricevitorie e tabaccherie Sisal: garanzie per la raccolta e il trattamento dei dati" del 15 Dicembre 2011 [doc. web n. 1883880]).

Inquadramento normativo e definizioni (3/3)

RICHIAMI NORMATIVI E DEFINIZIONI (3/3)

DEFINIZIONI UTILI

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 (nel nostro caso la banca) → art. 4 c. 7 e 24 GDPR

Responsabile della Protezione Dati o Data Protection Officer (DPO), che sorveglia l'osservanza del GDPR in azienda

Persone autorizzate al trattamento, già conosciuti come incaricati del trattamento (i dipendenti) → art. 29 GDPR

Referente privacy (Responsabile di U.O.) che assicura conformità normativa nella U.O. coordinata → art. 2-quaterdecies Codice privacy

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 → art. 4 c. 12 GDPR

Adempimenti in filiale: resa della informativa (1/3)

INFORMATIVA *PRIVACY*: LA NORMA

La normativa sulla protezione dei dati personali prescrive l'obbligo di rendere agli interessati (es. clienti e soggetti assimilati, quali i coobbligati) che conferiscono direttamente al titolare del trattamento (banca) i propri dati personali la **informativa** ai sensi dell'art. 13 del GDPR «*nel momento in cui i dati personali sono ottenuti*».

Il principio di responsabilizzazione (art. 24 GDPR) pone altresì in capo al titolare del trattamento l'obbligo di mettere in atto misure tecniche e organizzative adeguate per garantire, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al presente regolamento.

Adempimenti in filiale: resa della informativa (2/3)

Cfr. Regolamento UE 2018/1807 su dati non personali

esempio

INFORMATIVA *PRIVACY*: ADEMPIMENTO IN FILIALE

A seconda della tipologia di richiesta sono rese al cliente (e ai suoi eventuali coobbligati) informative diverse quali:

Informativa generale alla clientela	all'apertura del rapporto (mod …) [anche nel caso di **persone giuridiche** mod …]
Informativa SIC (mod …) e, in caso di mancato accoglimento (mod …)	alla richiesta di credito (finanziamento, carta di credito)
Informativa firma grafometrica	all'adesione al servizio

L'informativa relativa al trattamento delle immagini riprese dal sistema di videosorveglianza è esposta in forma sintetica (vetrofania) e disponibile anche sul sito della banca, in forma estesa.
Quando i dati non sono ottenuti presso l'interessato bensì pervengono da terzi, la resa dell'informativa non si applica nel caso che detto ottenimento[1] sia necessario per obbligo di legge (Art. 14 c. 5 GDPR).

Adempimenti in filiale: resa della informativa (3/3)

INFORMATIVA *PRIVACY*: RACCOMANDAZIONI

Per rispettare il principio di responsabilizzazione, è necessario conservare la informativa (nella versione vigente al momento in cui è resa) unitamente al modulo di consenso firmato dall'interessato attestando così il corretto adempimento della prescrizione normativa.
Per la informativa SIC, che non prevede il consenso (in quanto la base giuridica del trattamento è il legittimo interesse della banca), occorrerà far firmare e datare all'interessato copia della informativa resa che sarà conservata nel dossier cliente.

! *La mancata archiviazione del modulo di informativa/consenso, sebbene risultino valorizzati, nella specifica procedura, i consensi espressi dal cliente, non consente tuttavia alla banca di provarne l'avvenuto rilascio, con le conseguenze che ne derivano, anche in termini di trattamento per attività promozionali (vedi successiva slide n. 8). Per quanto ovvio, quanto censito relativamente ai consensi espressi dal cliente dovrà corrispondere, anche temporalmente, a quanto registrato nel modulo di informativa/consenso* ***archiviato*** *nel dossier cliente.*

In alcune banche i documenti sono digitalizzati

Adempimenti in filiale: raccolta del consenso (1/4)

CONSENSO: LA NORMA

Per alcuni trattamenti, quali quelli derivanti da **attività promozionali** nonché quelli relativi a dati appartenenti a **particolari categorie**(1) (quali i dati sulla salute, che potrebbero essere inseriti nella causale di un bonifico ad una struttura sanitaria o i dati biometrici necessari nell'adesione del cliente al servizio di firma grafometrica, rilasciata su tablet) è necessario raccogliere(2) il **consenso** che è costituito da una manifestazione di volontà:

- ✓ libera [scelta non condizionata (art. 7 c. 4 GDPR), possibilità di rifiutare e revocare senza pregiudizio);
- ✓ specifica (espresso per singola finalità);
- ✓ informata [almeno su identità titolare e finalità del trattamento (considerando 42 GDPR)];
- ✓ inequivocabile [mediante una **azione positiva** quale una dichiarazione scritta, distinguibile da altri aspetti, o verbale (registrata)]

(1) A questa tipologia di dati personali (art. 9 GDPR) appartengono dati già conosciuti come dati sensibili
(2) Il titolare del trattamento deve essere in grado di dimostrare di avere raccolto il consenso (art. 7 c. 1 GDPR)

Adempimenti in filiale: raccolta del consenso (2/4)

CONSENSO: ADEMPIMENTO IN FILIALE

Il consenso viene richiesto dalla banca alla clientela [anche alle persone giuridiche[1]] per i trattamenti:

Relativi ad attività di promozione commerciale

- ✓ promozione prodotti banca
- ✓ *customer satisfaction*
- ✓ promozione mirata attraverso profilazione
- ✓ promozione di prodotti di terzi (es. assicurativi)
- ✓ promozione da parte di terzi cui vengono ceduti i dati

di particolari categorie di dati

di dati biometrici acquisiti tramite firma del cliente su tablet

! In caso di cointestazione, il consenso va richiesto a ciascun cointestatario persona fisica e registrato sugli NDG dei singoli

(1) Le persone giuridiche in quanto contraenti di un contratto di telefonia possono rientrare nella disciplina del telemarketing (Registro Pubblico delle Opposizioni) di recente (luglio 2022) rinnovata

Adempimenti in filiale: raccolta del consenso (3/4)

CONSENSO: RACCOMANDAZIONI

Si sottolinea l'importanza di archiviare correttamente e tempestivamente i moduli recanti i consensi della clientela con particolare riferimento ai trattamenti per finalità di marketing, al fine di consentire alla banca, ove positivi, di dispiegare la propria azione commerciale nella maniera più completa.

L'azione di promozione commerciale può essere condotta verso la numerazione telefonica e gli indirizzi, di posta cartacea ed elettronica, comunicati dal cliente all'apertura del rapporto, o successivamente da lui modificati, e non verso numerazioni eventualmente acquisite per altre finalità (es. ricarica telefonica attraverso il conto corrente).

Adempimenti in filiale: raccolta del consenso (4/4)

CONSENSO: APPROFONDIMENTO

Art. 130 comma 4 del Codice privacy

*«Se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, **le coordinate di posta elettronica** fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, **può non richiedere il consenso dell'interessato**, sempre che si tratti di **servizi analoghi a quelli oggetto della vendita** e **l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni**. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente*

Art. 5 comma 1 della legge 5/2018

«Con l'iscrizione al registro(*) di cui al comma 2 si intendono revocati tutti i consensi precedentemente espressi, con qualsiasi forma o mezzo e a qualsiasi soggetto, che autorizzano il trattamento delle proprie numerazioni telefoniche fisse o mobili effettuato mediante operatore con l'impiego del telefono per fini di pubblicità o di vendita ovvero per il compimento di ricerche di mercato o di comunicazione commerciale ed è altresì precluso, per le medesime finalità, l'uso delle numerazioni telefoniche cedute a terzi dal titolare del trattamento sulla base dei consensi precedentemente rilasciati. **Sono fatti salvi i consensi prestati nell'ambito di specifici rapporti contrattuali in essere, ovvero *cessati da non più di trenta giorni,* aventi ad oggetto la fornitura di beni o servizi**, per i quali è comunque assicurata, con procedure semplificate, la facoltà di revoca»

(*) Si riferisce al Registro Pubblico delle Opposizioni

Adempimenti in filiale: riscontro esercizio diritti (1/5)

ESERCIZIO DEI DIRITTI: LA NORMA

Il GDPR garantisce all'interessato una serie di diritti stabiliti dagli artt. 7 c. 3 (revoca del consenso), da 15 a 22 (accesso, rettifica, cancellazione e portabilità dei dati nonché opposizione e limitazione del trattamento), 34 (comunicazione data breach) e 77 (reclamo all'Autorità di controllo).

Ad una richiesta di esercizio dei diritti deve essere dato riscontro entro un mese (art. 12) dalla ricezione della richiesta, con possibilità di proroga di due mesi, tenuto conto della complessità e numero delle richieste, che va comunque motivata al richiedente entro un mese dalla ricezione suddetta.

Le banche tipicamente ricevono richieste di esercizio dei diritti finalizzate a:

- cancellazione dei dati del richiedente dai SIC
- accesso ai dati (soprattutto movimentazioni) di persone decedute(1)
- ottenimento di documentazione contrattuale (e a tal proposito si segnala che lo smarrimento di documentazione contrattuale contenente dati personali può configurare un data breach da notificare al Garante privacy)
- revoca dei consensi marketing

(1) Il GDPR non si applica ai dati personali delle persone decedute (Considerando 27) ma gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute (art. 2-terdecies Codice privacy)

Adempimenti in filiale: riscontro esercizio diritti (2/5)

RICHIESTA ESTRATTI CONTO: APPROFONDIMENTO

Sovente le banche ricevono richiesta di fornire **gratuitamente**(1) copia degli estratti conto degli ultimi dieci anni (specialmente in caso di successione) ai sensi della normativa sulla protezione dei dati personali.

Occorre precisare che i dati forniti a sensi della normativa sulla protezione dei dati personali **sono quelli riferiti all'interessato e non a soggetti terzi**(2). **La copia integrale degli estratti conto può essere invece richiesta ai sensi del TUB**(3) ma «… a proprie spese …».

(1) «Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite.» (art. 12 c. 5 GDPR)

(2) «3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento …. 4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.» (art. 12 c. 3 e 4 GDPR)

(3) «Il cliente, colui che gli succede a qualunque titolo e colui che subentra nell'amministrazione dei suoi beni hanno diritto di ottenere, a proprie spese, entro un congruo termine e comunque non oltre novanta giorni, copia della documentazione inerente a singole operazioni poste in essere negli ultimi dieci anni. Al cliente possono essere addebitati solo i costi di produzione di tale documentazione.» (art. 119 c. 5 TUB)

Adempimenti in filiale: riscontro esercizio diritti (3/5)

RICHIESTA ESTRATTI CONTO: APPROFONDIMENTO

Sul punto il Garante privacy si è espresso qualche anno fa (in vigenza della previgente normativa italiana) in una linea guida di disciplina del trattamento dei dati della clientela bancaria[1] «*Il diritto di accedere ai dati personali previsto dall´art. 7 del Codice* ***deve essere distinto dal diritto di accesso alla documentazione bancaria previsto dall´art. 119 del Tub****. Va al riguardo considerato che quest´ultimo, a differenza di quanto previsto dagli artt. 7 ss. del Codice, riconosce al cliente, a colui che gli succede a qualunque titolo e a chi subentra nell´amministrazione dei suoi beni, il diritto di ottenere copia di atti o documenti bancari (sia che essi contengano dati personali relativi all´interessato, sia nel caso in cui ciò non accada)* ***Tale diritto non prevede limitazioni rispetto all´ostensibilità delle informazioni contenute nella documentazione richiesta (ivi compresi dati personali relativi a terzi che dovessero esservi contenuti),*** *neanche nelle forme di un parziale oscuramento delle informazioni stesse; il suo esercizio prevede il pagamento delle spese a carico del cliente … omissis …* ***informazioni che siano dati personali riferibili non all´interessato, ma a terzi non possono, invece, formare oggetto di comunicazione ai sensi degli artt. 7 e 9, comma 3, del Codice …»***

(1) "Linee guida per trattamenti dati relativi al rapporto banca-clientela" - 25 ottobre 2007

Adempimenti in filiale: riscontro esercizio diritti (4/5)

ESERCIZIO DEI DIRITTI: ADEMPIMENTO IN FILIALE

Nella informativa alla clientela della banca sono indicate le modalità di esercizio dei diritti

INSERIRE TESTO DA INFORMATIVA CLIENTI

Il riscontro delle richieste di esercizio dei diritti è disciplinato da ……..

INSERIRE TESTO DA REGOLAMENTO/POLICY AZIENDALE

Adempimenti in filiale: riscontro esercizio diritti (5/5)

ESERCIZIO DEI DIRITTI: RACCOMANDAZIONI

In considerazione della severità del quadro sanzionatorio che accompagna il GDPR (la violazione degli adempimenti mostrati in questo corso può comportare una **sanzione, fino a 20 milioni di euro** o fino al 4% del fatturato totale mondiale annuo dell'esercizio precedente se superiore) e della brevità del termine prescritto per il riscontro, riveste la massima importanza la **tempestività con cui si invia al DPO una richiesta di esercizio dei diritti pervenuta in Filiale**.

Protezione dei dati: comunicazione indebite (1/2)

COMUNICAZIONI INDEBITE DI DATI PERSONALI

3.2. **Comunicazioni indebite.** La comunicazione indebita di dati a terzi (che comporta gravi conseguenze anche sul piano della responsabilità civile e penale, alla luce degli artt. 15 e 167 del Codice) può avvenire per una pluralità di ragioni. Ciò può avvenire, a titolo meramente esemplificativo e tenendo in considerazione le tipologie di segnalazioni e ricorsi pervenuti all´Autorità, nei seguenti casi:

- per la mancata predisposizione di misure idonee a prevenire l´indebita conoscenza di informazioni personali da parte di terzi, ivi comprese le "**distanze di cortesia**" nei luoghi dedicati all´esecuzione di operazioni bancarie;
- per l´inosservanza delle istruzioni impartite agli incaricati del trattamento, come nel caso di **telefonate o colloqui effettuati indebitamente ad alta voce in presenza di terzi** [15];
- a seguito della **comunicazione di informazioni bancarie a terzi che non siano in alcun modo autorizzati dall´interessato** a porre in essere operazioni per suo conto o a conoscere il contenuto della relazione contrattuale in essere con la banca, come, ad esempio, nei confronti:
  - del **coniuge, cui venga consegnata documentazione bancaria riferita esclusivamente all´altro**;
  - di **familiari, contattati talora telefonicamente per comunicazioni dirette ai clienti, ma il cui contenuto venga invece rivelato ingiustificatamente ai primi**;
  - di professionisti o soggetti legati da un rapporto di lavoro con l´interessato;
  - di **terzi che, per errore nell´imbustamento o nella spedizione della corrispondenza, divengano destinatari di comunicazioni scritte aventi ad oggetto informazioni bancarie** (ad esempio, di estratti conto);
- a seguito della comunicazione di informazioni bancarie presso recapiti non autorizzati, in modo da consentire a terzi di venire a conoscenza di dati riferiti all´interessato (ad esempio, in caso di comunicazioni via fax)
- più in generale, per l´inosservanza di misure di sicurezza

Richiamo al punto 3.2 «Comunicazioni indebite» del provvedimento del Garante «Linee guida in materia di trattamento di dati personali della clientela in ambito bancario»

Protezione dati: disciplina accesso a dati bancari 2/2)

TRACCIAMENTO DELLE OPERAZIONI BANCARIE

Richiamo alla informativa al personale resa al momento dell'entrata in vigore (30 settembre 2014) del provvedimento del Garante privacy «Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie» del 12 maggio 2011, che prevede anche un accordo sindacale

Agenda

- Presentazione relatore
- L'importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- **Bibliografia & sitografia**
- Q&A

Bibliografia & Sitografia

Obblighi di formazione
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522 (Linee guida internet e posta elettronica)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9152344 (Manuale per RPD)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499 (Amministratori di sistema)

Informativa e consenso
https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1807&from=IT (Regolamento UE su dati non personali)
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9141941 (Codice di condotta SIC)
https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_it.pdf (Linee guida EDPB videosorveglianza)

Riscontro esercizio diritti e comunicazioni indebite
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247 (Linee guida trattamento dati clienti banca)

Disciplina accesso ai dati bancari della clientela
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953 (Tracciamento operazioni bancarie)

Agenda

- Presentazione relatore
- L’importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Bibliografia & sitografia
- Q&A

Agenda

- Presentazione relatore
- L'importanza della formazione nella protezione dei dati personali
- Un esempio di formazione per la filiale bancaria
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it

Grazie...

Da informativa alla clientela di grande banca

INFORMATIVA NEI CONFRONTI DI PERSONE GIURIDICHE, ENTI O ASSOCIAZIONI

Se rappresenti una persona giuridica, un ente o una associazione, ti informiamo che il consenso è necessario per autorizzarci all'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore e di comunicazioni elettroniche (posta elettronica, SMS, MMS o di altro tipo) per lo svolgimento di attività promozionale o il compimento di ricerche di mercato.

Il rilascio del consenso autorizza la Banca ad effettuare il medesimo trattamento anche mediante posta cartacea o chiamate telefoniche tramite operatore.

Aggiornata il 17.02.2023

Orientamenti Commissione UE (Reg. 2018/1807)

5. **Cosa sono gli insiemi di dati misti?**

Nella maggior parte delle situazioni reali, è molto più probabile che un insieme di dati sia composto da dati personali e non personali. In questo caso si parla spesso di "insieme di dati misti". Gli insiemi di dati misti rappresentano la maggioranza degli insiemi di dati impiegati nell'economia dei dati e sono comunemente raccolti grazie a sviluppi tecnologici come l'Internet degli oggetti (ossia dispositivi con connessione digitale), l'intelligenza artificiale e le tecnologie che consentono l'analisi dei big data.

I documenti fiscali di un'impresa, che indicano il nome e il numero di telefono dell'amministratore delegato della società, sono esempi di insiemi di dati misti. Possono anche consistere in insiemi di problemi e soluzioni informatici di un'impresa sulla base di segnalazioni individuali di incidenti, o in dati statistici anonimizzati di un istituto di ricerca e nei relativi dati grezzi inizialmente raccolti, quali le risposte dei singoli partecipanti alle indagini statistiche.

6. **I dati personali e i dati non personali devono essere trattati separatamente?**

No. Né il regolamento FFD né l'RGPD impongono l'obbligo di separare gli insiemi di dati misti o di trattare dati personali e dati non personali separatamente; in molti casi operazioni di questo tipo sarebbero problematiche e poco pratiche, se non addirittura impossibile. Gli orientamenti spiegano quindi le norme applicabili conformemente al regolamento FFD (articolo 2, paragrafo 2), mentre nel caso degli insiemi di dati misti:

- il regolamento FFD si applica alla parte dell'insieme costituita da dati non personali;
- le disposizioni sulla libera circolazione dell'RGPD si applicano alla parte dell'insieme costituita da dati personali.

Se le due parti sono "indissolubilmente legate", i diritti e gli obblighi in materia di protezione dei dati derivanti dall'RGPD si applicano integralmente all'insieme dei dati misti, anche nei casi in cui i dati personali rappresentano solo una piccola parte dell'insieme di dati.

Gli orientamenti illustrano anche il concetto di "indissolubilmente legato" e forniscono esempi concreti di applicazione di queste norme.