CYBER SECURITY

UNIVERSITÀ DI PARMA

DATA PROTECTION • CONSULTING • SECURITY

DATACONSEC

www.dataconsec.com

«La gestione tecnico organizzativa di un data breach: un caso pratico»

Domenico Carnicella, Alessandro Rodolfi, Roberto Tanara - Parma, 14 novembre 2019

DataConSec

Data Protection – Consulting – Security

- DataConSec
  - 1. Data Protection
    - 1.1 Gap Analysis GDPR
    - 1.2 Audit
      - 1.2.1 Misure organizzative
      - 1.2.2 Misure tecniche
    - 1.3 Adeguamento GDPR
    - 1.4 Data Protection Officer Outsourcing
    - 1.5 Data Protection Impact Assessment
    - 1.6 Adeguamento Sistemi CCTV
    - 1.7 Consulenza
    - 1.8 Formazione
  - 2. Consulting
    - 2.1 Sistemi di Gestione ISO
      - 2.1.1 Sicurezza informazioni 27001
      - 2.1.2 Business Continuity 22301
      - 2.1.3 Risk Management 31000
    - 2.2 Sistemi di Gestione 231/01
    - 2.3 Sistemi di Gestione AEO Dogane
    - 2.4 Adeguamenti Circolari Banca d'Italia
  - 3. Security
    - 3.1 Sicurezza informatica
      - 3.1.1 Servizi proattivi
        - 3.1.1.1 Security Assessment
        - 3.1.1.2 Vulnerability Assessment
        - 3.1.1.3 Penetration Testing
      - 3.1.2 Servizi gestiti
        - 3.1.2.1 Asset Management
        - 3.1.2.2 Continuos Monitoring
        - 3.1.2.3 Vulnerability Management
        - 3.1.2.4 Log Management
      - 3.1.3 Servizi reattivi
        - 3.1.3.1 Supporto allarmi di sicurezza
        - 3.1.3.2 Supporto incidenti di sicurezza
      - 3.1.4 Security Officer Outsourcing
      - 3.1.5 Consulenza
      - 3.1.6 Formazione
    - 3.2 Digital Forensics
      - 3.2.1 Raccolta prove da web
      - 3.2.2 Raccolta e analisi prove da PC e Server
      - 3.2.3 Raccolta e analisi prove da Tablet e Smartphone
      - 3.2.4 Raccolta e analisi prove da sistemi GPS e di videosorveglianza
      - 3.2.5 Recupero dati persi o cancellati in camera bianca
      - 3.2.6 Consulenza
      - 3.2.7 Formazione

La consulenza strategica, basata sull'analisi del ris
informazioni. Considerando la protezione dei dati cor
normativi, tecnologici e quelli organizzativi, l'approccio
rapportata all'esigenza del Cliente, valorizzando al mas

Il team di consulenti DataConSec, è composto da
esperienza nel mondo della sicurezza delle informazio

Consulenti legali
Privacy Officer
Consulenti di direzione aziendale
Auditor certificati
Digital Forensics Analyst accreditati in diverse Procure
ICT Security Expert
Security Manager

Le elevate competenze tecniche, l'etica professionale,
e manageriale, rappresentano una garanzia per il nost
delle informazioni trattate.
Lo staff è costantemente impegnato in attività di ricerca

Company Profile

DOMENICO CARNICELLA

PRIVACY, RISK AND COMPLIANCE

Lead Auditor ISO 27001 – 22301 – 9001
231/01 expert and AEO consultant

ALESSANDRO RODOLFI

PRIVACY, RISK AND COMPLIANCE

CISA - Lead Auditor ISO 27001 – 22301
Digital Forensics expert

Data breach: GDPR e linee guida

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Data security is at the heart of the upcoming General Data Protection Regulation

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679

adottate il 3 ottobre 2017

Versione emendata e adottata in data 6 febbraio 2018

Data breach: 9 ottobre 2018

Da: [redacted]
Inviato: martedì 9 ottobre 2018 07.53
A: GDPR
Oggetto: Richiesta annullamento profilo
Allegati: Screenshot_20181009-074955.jpg

Buongiorno
Ho ricevuto dei messaggi di spam da parte vostra (foto in allegato) . Non ho mai utilizzato i vostro sito e vi chiedo di annullare qualsiasi sottoscrizione riguardanti il trattamento di dati personali. Il mio numero è [redacted]
Vi ringrazio,
Buona giornata e buon lavoro

Da: [redacted]
Inviato: martedì 9 ottobre 2018 07.53
A: GDPR
Oggetto: Reclamo

Buongiorno, ho ricevuto un messaggio PRIVATO con su scritto di avere ricevuto un ipotetico rimborso in un mio ipotetico conto corrente in Deutschbank. Prima di tutto io non ho nessun conto corrente in nessuna banca, seconda questione io non voglio essere più contattato per queste o altre cose in merito! Ai fini di rispettare la mia richiesta e in forma legale le norme a tutela della privacy, mi auguro che DA SUBITO, ciò avvenga! !!

Quante persone sono state colpite dalla violazione?

- ☐ N. …….. persone
- X Presumibilmente 2.000 persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- X Numero di telefono mobile
- ☐ Indirizzo di posta elettronica
- X Dati anagrafici
- ☐ Dati di accesso e identificazione (user name, password, cutomer ID, altro)
- ☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
- ☐ Dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale
- ☐ Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza
- ☐ Dati relativi a minori
- ☐ Dati genetici
- ☐ Dati biometrici

[redacted] | EVENTO VIOLAZIONE DATI PERSONALI | [redacted]

In data [redacted], alle ore 7.53 la Distribution List aziendale di [redacted], riceveva una email proveniente dall'indirizzo di posta elettronica [redacted] (allegato 1), con la quale veniva richiesto dell'autore della email, l'annullamento di ogni sottoscrizione riguardante il trattamento dei propri dati personali.

Alle ore 7.54 la medesima Distribution List riceveva una seconda segnalazione contenente un messaggio simile al primo (allegato 2), da parte dell'indirizzo di posta elettronica [redacted]

Alle ore 7.57 l'IT Director, [redacted], veniva informato di un potenziale rischio di Data Breach da parte del Customer Care Manager, [redacted], il quale comunicava di aver rilevato presso i provider esterni del servizio di Call Center, la ricezione ingiustificata di un elevato numero di telefonate di clienti e non-clienti di [redacted] che richiedevano chiarimenti rispetto alle comunicazioni ricevute via sms.

Di seguito si riporta, a titolo di esempio, uno *screenshot* di messaggi ricevuti dai clienti e dai non-clienti di [redacted] a mezzo SMS:

[redacted]

Al termine dell'incontro, alle ore 11.00, venivano definite le seguenti azioni:

1. Ogni dipartimento avrebbe chiamato i propri fornitori e chiesto loro se avessero subito un Data Breach sui propri database; con l'occasione della telefonata, ogni referente avrebbe chiesto l'indirizzo PEC a cui [redacted] avrebbe inviato una PEC a seguire;
2. Ogni dipartimento avrebbe dato a stretto giro conferma di aver avvisato tutti i propri fornitori e avrebbe dovuto riportare le loro risposte all'ufficio legale [redacted] che avrebbe provveduto ad inviare le PEC;

- Online content: avrebbe messo un banner sul sito [redacted] con il relativo avviso (allegato 3);
- Marketing:
    I. Avrebbe messo la medesima comunicazione su facebook (allegato 8),
    II. Avrebbe inviato una mail a tutto il db clienti con il testo condiviso in riunione (allegato 4);
- [redacted]
- [redacted]
- Legal:
    I. Avrebbe verificato la presenza o meno di tutte le Nomine a responsabile del trattamento dei dati,
    II. Avrebbe predisposto la denuncia-querela da presentare alla Polizia Postale,
    III. Avrebbe allineato il DPO,
    IV. Avrebbe risposto alle email arrivate sulla casella [redacted]
    V. Avrebbe inviato le PEC ai fornitori.
- Customer care: avrebbe gestito le chiamate arrivate al call center.

Data breach: informare gli interessati
Es. Sito internet aziendale

GDPR
Diritti degli interessati

[redacted]

ATTENZIONE: IN QUESTE ORE ALCUNI DI VOI CI HANNO SEGNALATO DI AVER RICEVUTO UN SMS DA [redacted] CON UN LINK PER RICEVERE UN PRESUNTO RIMBORSO.

[redacted] **NON È IL MITTENTE DI TALE SMS.**

PERTANTO INVITIAMO QUANTI ABBIANO RICEVUTO QUESTO MESSAGGIO AD **ELIMINARLO IMMEDIATAMENTE E A NON CLICCARE SUI LINK PRESENTI AL SUO INTERNO.**

Data breach: informare gli interessati

9/10/2018

Comunicazione importante

Allegato 4

[redacted]

Pagamenti sicuri con Mastercard e Visa - Reso flessibile - Consegna 3/5 giorni
Nessuna immagine?

COMUNICAZIONE IMPORTANTE

ATTENZIONE: IN QUESTE ORE ALCUNI DI VOI CI HANNO SEGNALATO
DI AVER RICEVUTO UN SMS DA [redacted]
CON UN LINK PER RICEVERE UN PRESUNTO RIMBORSO.

[redacted] **NON È IL MITTENTE DI TALE SMS.**
PERTANTO INVITIAMO QUANTI ABBIANO RICEVUTO QUESTO MESSAGGIO AD
ELIMINARLO IMMEDIATAMENTE E A NON CLICCARE
SUI LINK PRESENTI AL SUO INTERNO.

Seguici sui nostri social

Garante per la protezione dei dati personali

N. [redacted] Roma, [redacted] 2018

ORDINE DI SERVIZIO

PER LA RICHIESTA DI INFORMAZIONI E DI ESIBIZIONE DI DOCUMENTI E L'EFFETTUAZIONE DI ACCESSI A BANCHE DI DATI, ISPEZIONI, VERIFICHE E ALTRE RILEVAZIONI *EX* ARTT. 157 E 158 DEL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196 *(artt. come sostituiti dall'art. 14, comma 1, lett. g) ed h) del d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679")*

Il Dipartimento attività ispettive è incaricato di effettuare gli accertamenti previsti dall'art. 58, comma 1, lettera a), e) ed f), del *"Regolamento generale sulla protezione dei dati (UE) 2016/679"* e dagli artt. 157 e 158 del d.lgs. n. 196/2003, recante il Codice per la protezione dei dati personali (di seguito "*Codice*"), nei confronti di:

- [redacted] *S.p.a.* [redacted] *con sede legale in* [redacted]

ordine di servizio, che potrà quindi effettuare gli accessi alle banche dati, nonché le altre ispezioni e verifiche nei luoghi ove si svolge il trattamento dei dati personali o nei quali occorre effettuare rilevazioni comunque utili al controllo.

La dichiarazione di assenso informato sottoscritta dall' [redacted] viene allegata al presente verbale.

I verbalizzanti hanno provveduto a informare la parte che i soggetti presso i quali sono eseguiti gli accertamenti di cui all'art. 158 del Codice sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento (art. 159, comma 2, del Codice).

Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile del trattamento (art. 159, comma 3, del Codice).

I verbalizzanti, altresì, hanno resa edotta la parte delle conseguenze penali che l'art. 168 del *Codice* riconduce a *[...] chiunque in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, con la reclusione da sei mesi a tre anni [...]* nonché, *[...] è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti [...].*

Alle operazioni partecipano, in qualità di intervenuti:

- ✓ *dott. Alessandro Rodolfi, R.p.d.* [redacted] *(socio "Dataconsec S.r.l." di Parma);*
- ✓ *dott.* [redacted] *Customer care* [redacted] *;*
- ✓ *dott.ssa* [redacted] *Responsabile Area marketing* [redacted] *;*
- ✓ *dott.* [redacted] *Direttore I.T.* [redacted] *.;*
- ✓ *dott.ssa* [redacted] *Responsabile C.r.m.* [redacted] *;*
- ✓ *dott.ssa* [redacted] *Junior legal specialist* [redacted]
- ✓ *dott.* [redacted] *Responsabile Area Amministrativa* [redacted]

Art. 157 Richiesta di informazioni e di esibizione di documenti

1. *Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti* ***anche con riferimento al contenuto di banche di dati****.*

[Art. 58 del Regolamento > I **poteri** delle autorità di controllo sono **molto ampi**]

Art. 158 Accertamenti #1

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei **luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni** comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1, nonchè quelli effettuati ai sensi dell'articolo 62 del Regolamento [*operazioni congiunte*], sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea.

3. Il Garante si avvale anche, ove necessario, della **collaborazione di altri organi dello Stato** per lo svolgimento dei suoi compiti istituzionali.

Art. 158 Accertamenti #2

4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con **l'assenso informato** del titolare o del responsabile, oppure **previa autorizzazione del presidente del tribunale competente per territorio** in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

5. Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresì riguardare **reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on-line**. A tal fine viene redatto apposito verbale in contradditorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento.

Linee guida data breach WP250

Se il titolare del trattamento omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'imposizione di una sanzione amministrativa pecuniaria appropriata[19], in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure come sanzione indipendente. Qualora l'autorità opti per una sanzione amministrativa pecuniaria il suo valore può ammontare fino a un massimo di 10 000 000 EUR o fino al 2% del fatturato totale annuo globale di un'impresa ai sensi dell'articolo 83, paragrafo 4, lettera a), del regolamento. È altresì importante ricordare che, in alcuni casi, la mancata notifica di una violazione potrebbe rivelare l'assenza di misure di sicurezza o la loro inadeguatezza. Gli orientamenti del Gruppo di lavoro in materia di sanzioni amministrative affermano che "qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti

[17] Cfr. anche considerando 85 e 75.

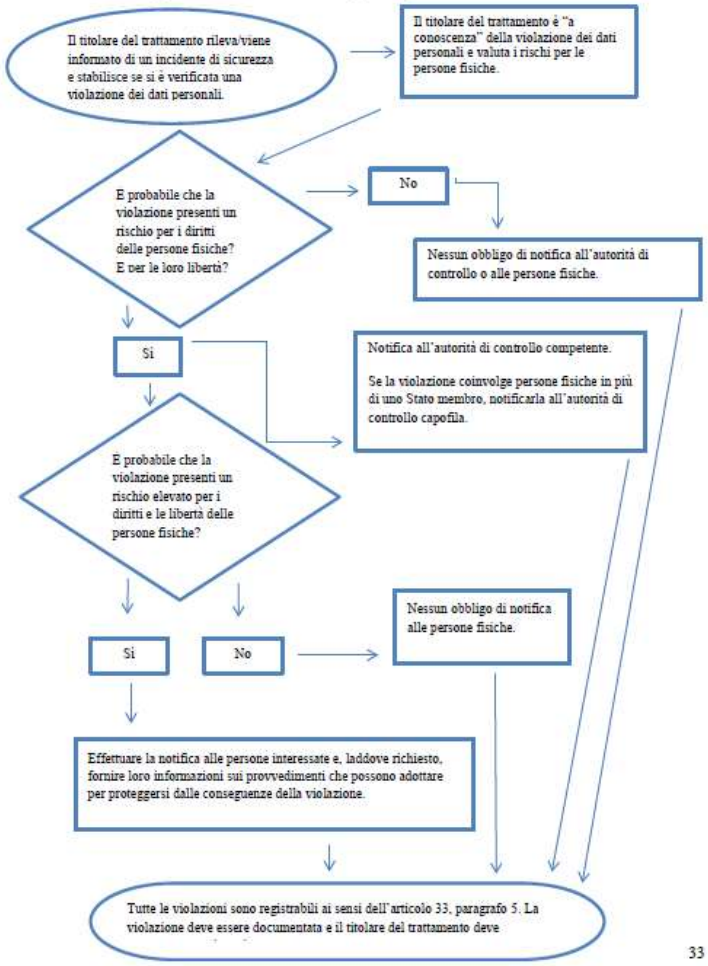
[18] Cfr. anche il considerando 86.

[19] Per ulteriori dettagli, consultare le linee guida del Gruppo di lavoro riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie disponibili qui: https://www.garanteprivacy.it/documents/10160/0/WP+253++Linee+guida+sanzioni+amministrative+pecuniari

Le verifiche GdF: oggetto e presupposti

Modalità: Linee guida data breach

A. Diagramma di flusso che illustra gli obblighi di notifica



33

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

○ Preliminare[1]	○ Completa	◉ Integrativa [2]	rif.
Effettuata ai sensi del	◉ art. 33 RGPD	○ art. 26 d.lgs 51/2018	

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.

2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)

2. Notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Gestire « *IT management* » un potenziale Data Breach

1. Misure di sicurezza adeguate al livello di rischio
2. Competenze + formazione continua
3. Visibilità sugli strumenti che trattano i dati
4. Monitoraggio degli eventi + threat intelligence
5. Individuazione + analisi + contenimento + rimedio degli incidenti
6. Documentazione e miglioramento continuo

DATA PROTECTION • CONSULTING • SECURITY

DATACONSEC

Sede legale e amministrativa:
V.le Fratti, 56 Parma - Italia

Tel. e Fax: +39 0521 77 12 98

P.IVA/C.F.: 02470920345

www.dataconsec.com

info@dataconsec.com
amministrazione@pec.dataconsec.com

Social