GDPR

Attacco ransomware contro l'Ospedale Fatebenefratelli di Erba: 35mila radiografie inaccessibili

Un attacco **ransomware** ha congelato per giorni le attività dell'Ospedale Fatebenefratelli di Erba e come se non bastasse **più di 35mila radiografie sono state rese inaccessibili**. La dirigenza sanitaria, come ha raccontato venerdì scorso l'edizione di Como del quotidiano Il Giorno, ha deciso di non rispondere alla richiesta di riscatto e quindi procedere con denuncia contro ignoti. Come vuole la prassi si occuperà del caso la Divisione Distrettuale di Milano specializzata in reati informatici.

Dove sono i dati personali

- La civiltà della sorveglianza
  - Telecamere intelligenti, rilevazioni biometriche, *RFID*, sistemi di localizzazione, IOT, ecc.
- Noi siamo le tracce che lasciamo
  - Crescono quanto più i servizi sono sofisticati
  - Cloud evoluto
- L'identità costruita sulla base di esse
  - Intelligenza artificiale e Machine learning

Lo sviluppo delle banche dati

- Sviluppo tecnologico e conservazione dei dati
  - Aumenta la capacità di memoria
  - Si accrescono i tempi di conservazione
  - Si moltiplicano le interconnessioni fra banche dati
  - Diventa meno costoso conservare i dati
    - Un esempio: i motori di ricerca

Memoria e oblio

- Diritto all'oblio come diritto di libertà
  - Di scegliere liberamente
  - Di cambiare e di correggersi (Identità)
- I nemici dell'oblio
  - Le capacità tecniche di conservazione dei dati
  - La nostra pigrizia
- La sentenza Google Spain
- Il nuovo Regolamento
- Oblio e sicurezza
  - Dalla contrapposizione alla complementarietà

Perché valgono tanto

- Rischi di sottovalutazione
  - Non è un gioco da ragazzi
  - Non è virtuale
- Il valore dei dati
  - Economico
    - Dopo l'oro giallo e l'oro nero…la profilazione
  - Strategico
    - La nuvola europea
    - Verso un Privacy Schield
  - Sicurezza: criminalità comune e organizzata
  - Politica: dalla consultazione permanente alla profilazione degli elettori

Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)

II EDIZIONE 2018

Disciplina generale

Dal Codice Privacy al Regolamento generale UE

Una normativa in continua evoluzione

- Le leggi 31 dicembre 1996, nn. 675 e 676 e le successive deleghe
  – Dal diritto ad essere lasciati soli al controllo sui propri dati
- I decreti delegati fino al d.lgs. 467/2001
- Gli atti paranormativi e le pronunce del Garante
- **Il Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196)**

La mappa del Codice privacy

- **Parte I: Disposizioni generali**
- **Parte II: Disposizioni relative a specifici settori**
  - Trattamenti in ambito giudiziario (artt. 46 ss.)
  - Trattamento da parte di forze di polizia (artt. 53 ss)
- **Parte III: Tutela dell'interessato e sanzioni**

Allegati

- A) I Codici deontologici
- B) Disciplinare tecnico in materia di misure minime di sicurezza
- C) Trattamenti in ambito giudiziario e per fini di polizia (vedi slides seguenti)

I pilastri della tutela

(Codice Privacy)

- Informativa
- Consenso
- Autorizzaziome
- Base normativa per soggetti pubblici (v. seguente)
  - Diritti dell’interessato
  - Misure di sicurezza
- Notificazione
  - Differenze col Regolamento Generale (rinvio)

Corso di alta formazione sulla Protezione dei Dati Personali per Responsabile della protezione dei dati (DPO)

II EDIZIONE 2018

Disciplina generale – Dal Codice Privacy al GDPR

Dati personali e loro tipologie

I dati personali nella normativa italiana

- Qualunque informazione relativa a:
  - **persona fisica**
  - *[persona giuridica, ente od associazione]*
    - *DL n. 201/2011, (convertito in legge n. 214/2011)*
- Identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale

I dati personali nel GDPR

- Qualsiasi informazione
- Riguardante una **persona fisica**
- Identificata o identificabile («interessato»)
-

La figura dell'interessato

- Idendificabilità (rinvio)

Quando una persona è identificabile?

- Quando la persona fisica può essere identificata, direttamente o indirettamente
  - con particolare riferimento a un identificativo 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

La Pseudonimizzazione

- 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

I dati sensibili nel Codice privacy

- Il “nocciolo duro” della riservatezza

  Quelli idonei a rivelare (art.4, comma 1,lett.d)**:**
  - l’origine razziale ed etnica,
  - le convinzioni religiose, filosofiche o di altro genere nonché le opinioni politiche,
  - l’adesione **a partiti,** sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale,
  - lo stato di salute o la vita sessuale

  Evitare le interpretazioni troppo estensive

Categorie particolari di dati personali (art. 9)

- 1. È vietato trattare dati personali che rivelino:
  - l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati **genetici**, dati **biometrici** intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

(Rinvio sul regime applicabile)

I dati relativi alla salute nel GDPR

- 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

I dati biometrici nel GDPR

- I dati personali ottenuti da un trattamento tecnico specifico relativi alle **caratteristiche**
  - **fisiche,**
  - **fisiologiche**
  - **o comportamentali**
- che consentono o confermano l'**identificazione univoca** di una persona fisica
  - quali l'immagine facciale o i dati dattiloscopici

I dati genetici nel GDPR

- I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

Figure soggettive

Figure Soggettive

- **Titolare del trattamento**
- **Responsabile del trattamento**
- **Contitolari del trattamento**
- **Rappresentanti di titolari**
- **Subresponsabile**
- **Obblighi e responsabilità**
- **Registri del trattamento**

...

un gioco di squadra !

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

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

Contitolarità del trattamento

- Quando “**determinano congiuntamente le finalità e i mezzi del trattamento”**
- determinano in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento
- Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato
- L'interessato può esercitare i **propri diritti** nei confronti di e contro ciascun titolare del trattamento

Responsabile del trattamento

- Chi può essere responsabile del trattamento?
- Soggetti che presentino garanzie sufficienti per **mettere in atto** misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato
- Valutazione che deve essere condotta dal **titolare del trattamento**

Per conto del titolare

- Significa che il responsabilità del trattamento agisce per finalità non proprie, ma determinate dal titolare
- Ad esempio, la società Alfa incarica la società Beta di compiere una campagna marketing e le comunica il suo DB proprietario
- Se la società Beta utilizza il medesimo DB per un altro cliente, non sta agendo in qualità di responsabile del trattamento di Alfa

Responsabile “interno” ed “esterno”

- Il RGPD si applica solo ai responsabili “esterni” ossia ai soggetti che non sono legati da un rapporto di lavoro con il titolare?
- E’ possibile nominare del dei responsabili “interni”?
- E’ vietato nominare dei responsabili “interni”?
- Cosa dice la bozza di Decreto legislativo?
- È una misura di accountability?

Data Breach

WIRED.IT Sezioni Wired Next Fest Gallery Video

HOT TOPIC OLIMPIADI INVERNALI FACEBOOK DIZIONARIO DIGITALE ELEZIONI 2018 GOOGLE SERIE TV WIRED HEALTH SMARTPHONE... VEDI TUTTI

HOME ATTUALITÀ TECH

di Giuditta Mosca
19 AGO, 2015

Ashley Madison, online tutti i dati dei traditori

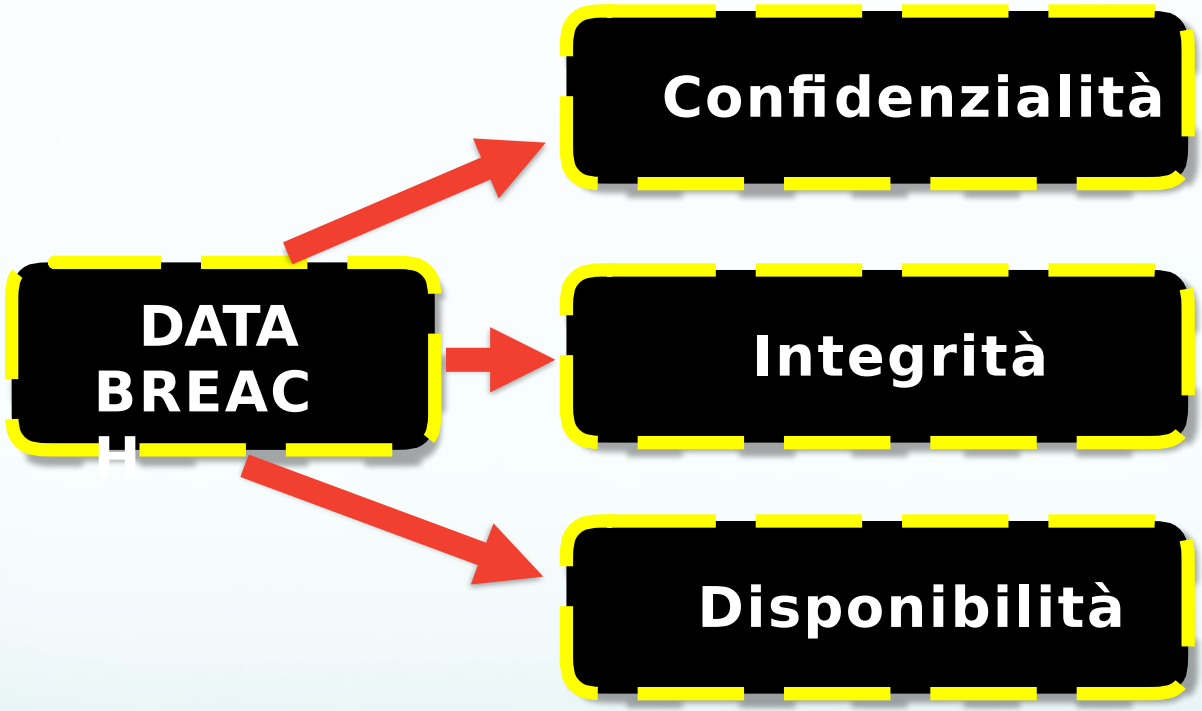
Lo scorso luglio un gruppo di hacker ha violato il famoso sito per adulteri, prelevando milioni di dati sensibili. Ora sono disponibili online

VIDEO

I dati di **milioni di fedifraghi** prelevati dal sito **Ashley Madison** lo scorso luglio sono online, nel file da **9,7 GB** si possono trovare i **nomi** degli utenti, i loro **indirizzi email**, **preferenze sessuali** e le transazioni avvenute tramite

Conseguenze estreme …

quali data breach?



Definizione di Data Breach (art. 4)

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso [non autorizzato] ai dati personali trasmessi, conservati o comunque trattati

Le cause frequenti dei data breach

Errore umano

Errori di configurazione Errori nella gestione Formattazione e dismissione Compromissione dei backup Danni da liquidi Imprudenze e negligenze

Attacchi

Accessi abusivi esterni/insiders Leak dei dati
Virus & Malware Social engineering Furti e danneggiamenti

Danni e hardware

Fornitura di energia Eventi naturali

roditori, funghi… incendi, allagamenti etc

Obsolescenza hardware e software

Art. 33: data breach nel GDPR

Notifica di una violazione dei dati personali all'autorità di controllo

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**.

Quando è improbabile il rischio derivante da data breach?

if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly ***encrypted personal data*** *may not need to be notified to the supervisory authority (WP29)*

Art. 33 GDPR

2. Il **responsabile del trattamento informa il titolare** del trattamento **senza ingiustificato ritardo** dopo essere venuto a conoscenza della violazione.

Questo ultimo obbligo va **specificato nell'accordo negoziale con il data processor**, ex art. 28, comma 3

[…] Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli ***articoli da 32 a 36****, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;*

Contenuto della notifica al Garante

3. La notifica di cui al paragrafo 1 deve almeno:

a)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** [records] dei dati personali in questione;

b)comunicare **il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto** presso cui ottenere più informazioni;

c)descrivere le **probabili conseguenze della violazione** dei dati personali;

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

Art. 34 - Comunicazione all'interessato

1. Quando la violazione dei dati personali è **suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato **senza ingiustificato ritardo**.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la **natura della violazione dei dati personali** e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

b) comunicare **il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto** presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

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

Art. 34 - Quando il rischio è “elevato”

La valutazione del rischio “elevato”: il considerando 75 (in stretto collegamento al considerando 85)

- il trattamento può comportare discriminazioni, furto o usurpazione d’identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, **o qualsiasi altro danno economico o sociale significativo**;
- se gli interessati rischiano di essere **privati dei loro diritti e delle loro libertà** o venga loro impedito l’esercizio del controllo sui dati personali che li riguardano;

Art. 34 - Comunicazione all'interessato

Modalità della comunicazione

- Messaggio specifico (no a inserimento in newsletter etc.)
- Comunicazione sul sito
- Eventuale pubblicazione su quotidiani e simili
- Attenzione al formato e alla lingua
- Attenzione ai phishing che simulano i data breach

Tempestività

è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge **[law-enforcement authorities]**, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali. (C.88)

Quando non è dovuta la comunicazione all'interessato

a) **il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà** degli interessati di cui al paragrafo 1;

c) **detta comunicazione richiederebbe sforzi sproporzionati**. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Responsabilità e Sanzioni

Rappresentanza degli interessati

Articolo 80

L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.

... ma dobbiamo tremare ...
o festeggiare ?

Risarcimento (Art. 82.6): Il risarcimento del danno è domandato dinanzi alle autorità giurisdizionali competenti. Le questioni risarcitorie non appaiono proponibili dinnanzi alle Autorità garanti.
L'interessato potrà sempre radicare, anche successivamente al reclamo, autonoma domanda risarcitoria.

Modalità e durata: predisposizione di modelli da parte delle Autorità garanti, anche elettronicamente, il cui utilizzo resta comunque meramente facoltativo.

- Il Regolamento non fissa la durata massima della procedura di reclamo, ma l'Autorità deve informare il reclamante entro "un termine ragionevole"
- Appare comunque corretto valorizzare il riferimento al trimestre, espressamente contenuto all'art. 78.2, quale unità temporale significativa, non come termine perentorio, ma nel senso che costituisce l'orizzonte temporale congruo affinché si pervenga a una definizione della procedura amministrativa.

Il Reclamo al Garante privacy (1)

- Il reclamo può essere sottoscritto direttamente dall'interessato oppure, per suo conto, da un avvocato, un procuratore, un organismo, un'organizzazione o un'associazione senza scopo di lucro. In tali casi, è necessario conferire una procura da depositarsi presso il Garante assieme a tutta la documentazione utile ai fini della valutazione del reclamo presentato.

- Il reclamante può far pervenire l'atto utilizzando la modalità ritenuta più opportuna, consegnandolo a mano presso gli uffici del Garante (all'indirizzo di seguito indicato) o mediante l'inoltro di:

a) raccomandata A/R indirizzata a Garante per la protezione dei dati personali, Piazza di Monte Citorio, 121 00186 Roma

b) messaggio di posta elettronica certificata indirizzata a protocollo@pec.gpdp.it

- In sede di prima applicazione, il reclamo e l'eventuale procura dovranno essere sottoscritti con firma autenticata, ovvero con firma digitale, ovvero con firma autografa (in tale ultimo caso, al reclamo dovrà essere allegata copia di un documento di riconoscimento dell’interessato/a in corso di validità).

La responsabilità civile del titolare o responsabile del trattamento

Art. 82(1), (2) e (3) – Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. **Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.**
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

Le sanzioni amministrative

►**Sanzione amministrativa pecuniaria fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni delle seguenti disposizioni del regolamento (art. 83, par. 5):**

- principi base del trattamento, comprese le condizioni del consenso (artt. da 5 a 7 e 9);
- diritti degli interessati (artt. da 12 a 22);
- trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale (artt. da 44 a 49);
- qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX del regolamento. Si tratta delle disposizioni che autorizzano gli Stati a dotarsi di una disciplina ulteriore con riferimento ai trattamenti che concernono la libertà di espressione e di informazione, ai trattamenti in ambito lavorativo, ai fini di archiviazione nel pubblico interesse;
- l'inosservanza di un ordine, di un provvedimento di limitazione del trattamento o di un ordine di sospensione dei flussi di dati adottato dall'autorità di controllo nell'ambito dei poteri correttivi (art. 58, par. 2);
- il diniego di accesso all'autorità di controllo che svolga poteri di indagine (art. 58, par. 1).

Il procedimento di applicazione delle sanzioni

I restanti commi dell’articolo 166 disciplinano il procedimento per l’applicazione delle sanzioni.

Ferma restando - in attuazione dell’art. 58, par. 4, del regolamento - l’adozione con regolamento del Garante delle specifiche modalità procedurali e i relativi termini per l’adozione dei provvedimenti correttivi e delle sanzioni indicate (comma 10), **viene stabilito che il contravventore, cui l’ufficio del Garante ha comunicato le presunte violazioni (comma 6), ha 30 giorni di tempo per inviare scritti difensivi o documenti, potendo chiedere di essere sentito in audizione (comma 7).**

Il procedimento di applicazione delle sanzioni

Il 50% delle sanzioni riscosse annualmente sono riassegnate al Fondo presso il Ministero dell'economia, previsto dal nuovo art. 156 del Codice per le spese di funzionamento del Garante.

Tanto l'applicabilità della legge n. 689/81, quanto la riassegnazione dei proventi delle sanzioni al Fondo per il funzionamento del Garante, sono già previsti dalla normativa vigente.

Al trasgressore è offerta la possibilità del pagamento della sanzione in misura ridotta. Il comma 9 dell'articolo 166 dispone infatti che - «entro il termine previsto per la proposizione del ricorso» il trasgressore possa definire la controversia pagando la metà della sanzione irrogata e adeguandosi alle prescrizioni del Garante.

LA NOSTRA SOLUZIONE

Cosa cambia per le aziende

Il **GDPR** introduce un ampio spettro di novità imponendo di **definire un piano di adeguamento alla nuova normativa**. **Tutte** le diverse **funzioni aziendali** che gestiscono e trattano dati personali sono coinvolte. Alcune di esse impongono un’attenta pianificazione poiché possono comportare modifiche organizzative importanti e investimenti di natura tecnologica, per questo l**a nuova normativa darà maggior risalto al team IT e ai CIO aziendali, conferendo un ruolo cruciale alle loro mansioni**. Il nuovo regolamento sarà causa di severe sanzioni per le aziende che non lo rispetteranno, ma le conseguenze non saranno solo economiche: il mancato rispetto delle nuove norme avrà anche **ripercussioni sulla reputazione e sull’immagine della compagnia**, che non verrà considerata come attenta alla privacy degli utenti e ai loro dati sensibili.

Come possiamo aiutarvi

L’avvento del GDPR segna un deciso “cambio di passo” nella gestione dei dati, per il quale si rende necessario **predisporre metodologie specifiche atte a monitorare in maniera “*compliant*”** tutti i dati soggetti a regolamentazione. Prima di affrontare il problema da un punto di vista tecnologico è importante capire lo stato dell’arte ovvero a che punto è la vostra azienda, **predisporre una “*roadmap*” evolutiva** e una conseguente crescita sulla cultura del dato che da questa rivoluzione è auspicabile attendersi. Supportiamo le aziende **in tutte le fasi critiche** che coinvolgono la **normativa GDPR**, partendo dalla progettazione e dagli audit di miglioramento, fino alla formazione.

L’offerta modulare

- Analisi del perimetro, dei processi e profilazione dei trattamenti
- Risk Analysis, DPIA, Security Assessment
- Modello di gestione, profilazione ruoli, creazione registri e informative
- Formazione, Awareness, Audit annuali, Servizio DPO esterno incluso
- Servizi di sicurezza gestita per la protezione dei dati personali

Certificazioni

- I nostri consulenti in materia GDPR che vi seguiranno nel percorso di formazione ed adeguamento sono certificati ISO 27001 (Security) e UNI 11697 (DPO).
- Inoltre siamo in grado di fornire soluzioni hardware e software per una corretta gestione della sicurezza informatica all’interno dell’Azienda, ovvero:

Strumenti di Autenticazione Forte

La soluzione di **DigitalPersona**® è progettata per fornire un insieme di fattori di autenticazione e per soddisfare i requisiti previsti dal GDPR per minimizzare il rischio di accessi non autorizzati e “data breach”. L’autenticazione composita rappresenta il giusto mix di autenticazione in ogni istante – definisci ciò che hai, che sei e che conosci - con l’analisi dei fattori di rischio contestuali di tempo, velocità, posizione e comportamento. Scegli il giusto livello di protezione per ogni applicazione, ogni utente e ogni sistema. Proteggi tutte le tue applicazioni, inclusi Web, Cloud, Windows, dispositivi mobili, VDI e VPN, persino le applicazioni “legacy” su mainframe che continuano a svolgere un ruolo fondamentale. Con **DigitalPersona**®, tutti i dipartimenti sono coperti – dipendenti, clienti, venditori e partner.

Strumenti di Autenticazione Forte

DigitalPersona® riesce quindi a combinare una vasta gamma di fattori per l'autenticazione aziendale, come quelli di seguito riportati a titolo di esempio:

- Qualcosa che hai: Smart, Proximity e Contactless Cards; Telefono Bluetooth
- Qualcosa che conosci: PIN, password, OTP
- Qualcosa che sei: biometria (viso, impronte digitali)
- Cosa fai: sequenza di tasti, scorrimento, tracciamento del mouse
- Dove ti trovi: posizione GPS, indirizzo IP….

L'adozione di dati biometrici ha visto un aumento vertiginoso negli ultimi anni, e per una buona ragione. Oltre ad essere una credenziale forte, è l'unico fattore di autenticazione che fornisce una "prova di presenza" ed il non ripudio. Recentemente una comunicazione del Garante Privacy ha autorizzato l’utilizzo della biometria per questioni di sicurezza, con alcune cautele tecniche e legali di cui la nostra consulenza in merito al GDPR saprà tenere conto.

Distruzione dei dati sensibili

La distruzione deve avvenire sia nel caso i dati siano contenuti su documenti cartacei sia nel caso siano contenuti su supporti magnetici (tramite Degausser) o su SSD. Possiamo offrire tutte le soluzioni utili per il raggiungimento di questo obiettivo.

La DISTRUZIONE, deve far si che il documento non sia più leggibile o ricostruibile, come confermato dall'ufficio garante privacy.

Per quanto riguarda invece la modalità e il grado di protezione per la determinazione della distruzione dei documenti si deve far riferimento alla **NORMA DIN 66399** che definisce le varie tipologie dei dati trattati e i requisiti che devono avere le macchine ed i processi impiegati nella distruzione.

GRAZIE PER L’ATTENZIONE

… e seguiteci su:

www.gdprpassport.it