Tutele sulla sicurezza fisica e la privacy previste dal regolamento GDPR

Il Regolamento GDPR (Regolamento generale sulla protezione dei dati) dell'Unione Europea richiede alle organizzazioni di tutto il mondo di ripensare le modalità di accesso, utilizzo e custodia dei dati personali. In questo White Paper vengono descritti gli scenari di rischio per i dati che, secondo il nuovo regolamento, potrebbero essere la causa di interventi amministrativi e di sanzioni pecuniarie. Il White Paper esamina inoltre le migliori prassi in termini di sicurezza fisica e privacy, in quanto queste rappresentano un aspetto importante, ma spesso trascurato, nel settore della protezione dei dati. La combinazione delle protezioni amministrative, informatiche e fisiche può contribuire a tutelare la sicurezza dei dati personali sensibili e dimostra l'impegno e il rigore di un'organizzazione nel campo della riservatezza dei dati.

Punti chiave:

- Approfondimento delle direttive del regolamento GDPR a proposito della sicurezza fisica e delle misure di protezione della privacy dei dati personali.
- Resoconto di ciò che gli esperti del settore considerano un ragionevole livello di protezione dei dati e della privacy.

Vivere in un mondo basato sui dati
Raccogliere e utilizzare i dati personali, sui dipendenti, sui clienti esistenti o potenziali o su altri soggetti, è una componente assolutamente normale delle attività di una impresa moderna. Tipicamente, i dati vengono memorizzati in forma elettronica per garantirne l'accesso sia all'interno dell'organizzazione[1] che da soggetti esterni. Inoltre, la funzione principale di alcune organizzazioni è specificamente quella di raccogliere e di analizzare grandi volumi di dati personali.

Anche se la quantità e il tipo di dati raccolti dalle organizzazioni variano sensibilmente, è opinione diffusa che la ricerca di tali dati non sia mai stata così facile. Le persone lasciano dietro di sé una traccia significativa di dati quando creano i profili dei social media, partecipano a comunità online, conducono ricerche su internet, rispondono ai sondaggi e approfittano di offerte promozionali e servizi "gratuiti", come ad esempio la memorizzazione di foto e la riproduzione in streaming di brani musicali.

La tecnologia contribuisce ulteriormente al processo di creazione di robusti profili sulle persone, grazie agli avanzamenti ottenuti in termini di intelligenza artificiale, e-tag, web beacon, cookie e altri strumenti di monitoraggio.

Insieme, la tecnologia e le iniziative di data mining hanno consentito alle organizzazioni di accumulare grandi insiemi di dati personali. Queste banche dati possono rivelare informazioni come l'età, lo stato civile, la data di nascita, il livello di istruzione, gli hobby, la religione, le esperienze lavorative, le convinzioni politiche, le preferenze di acquisto, le fonti di notizie preferite, il reddito, la fedina penale e molto altro ancora.

Anche se molti di questi dati sono centralizzati nei database dell'azienda, spesso esiste l'esigenza di rilasciare piccoli set di dati nei sistemi eterogenei della supply chain - che spesso non dispongono di meccanismi per comunicare ai futuri destinatari dei dati come o perché tali dati sono stati originariamente raccolti. Questo permette che i dati personali vengano esposti ad usi che si discostano dallo scopo originale per il quale sono stati ottenuti.

In un dato giorno, numerose persone all'interno di un'organizzazione possono accedere ai dati memorizzati - ad esempio per pagare un collaboratore, condurre ricerche di mercato, lanciare una campagna di marketing via e-mail o per tracciare il grado di coinvolgimento dei clienti. Ogni punto di accesso a questi set di dati rappresenta un'opportunità di utilizzo improprio o non autorizzato dei dati personali.

Informazioni rapide

Che cosa è il GDPR?
Il regolamento generale sulla protezione dei dati (GDPR) mira a proteggere la privacy delle persone residenti nell'Unione Europea (UE).

Quando entrerà in vigore?
Il 25 maggio 2018

Chi interessa?
Tutte le imprese - indipendentemente dalla loro ubicazione - che controllano o elaborano dati personali di persone residenti nell'Unione Europea.

Cosa s'intende con dati personali?
Qualsiasi informazione correlata a una persona fisica o soggetto interessato. I dati personali possono avere natura estremamente diversificata, da un nome, una foto, un indirizzo di posta elettronica, coordinate bancarie, post su siti di social network, informazioni mediche, o persino l'indirizzo IP di un computer.

Quali sono le conseguenze?
Le violazioni possono comportare un'ammenda pari a 20 milioni di euro o fino al 4 per cento del fatturato globale annuo dell'azienda (a seconda di quale sia la maggiore). Questa è la sanzione massima che può essere imposta per la maggior parte delle infrazioni gravi.

Dove posso trovare ulteriori informazioni?

- Una panoramica del regolamento
- Testo completo del regolamento
- Soluzioni di sicurezza fisica

Il 65% degli intervistati ritiene che gli incidenti di violazione dei dati abbiano fatto perdere loro la fiducia nell'organizzazione interessata.[5]

Per comprendere i rischi in termini di sicurezza fisica che le organizzazioni si trovano ad affrontare, consideriamo questi scenari:

Un dipendente esamina dati sensibili sul proprio telefono mentre si trova in aeroporto e non si accorge che qualcuno guarda il suo schermo.

- Un dipendente perde il proprio computer portatile e le informazioni sull'unità di memoria non sono crittografate.
- Un dipendente si allontana dalla propria scrivania per prendere un caffè, lasciando le informazioni di contatto del cliente visualizzate sul monitor o sulla scrivania mentre passa qualcuno che non è autorizzato alla loro visione.
- Un dipendente insoddisfatto scatta foto di documenti lasciati su una stampante, informazioni visualizzate su uno schermo o credenziali di accesso fissate con nastro adesivo al monitor di un computer.
- Computer portatili o desktop vengono donati ad enti di beneficenza senza cancellare completamente le unità di memoria.
- Un ambulatorio medico chiude e getta le cartelle dei pazienti nel cassonetto senza distruggerle con apposito tritadocumenti.

Nel 2016 gli hacker hanno compromesso **1 miliardo di record**[2]

Scenari come questi sono sempre più preoccupanti, in quanto le violazioni di dati sono fin troppo comuni nel moderno mondo digitalizzato. Forrester riporta che in soli dodici mesi nel 2016 gli hacker hanno compromesso un miliardo di record. Lo studio ha indicato che nella prima metà del 2017 con 918 violazioni di dati siano stati compromessi 1.9 miliardi di record di dati in tutto il mondo. Ciò rappresenta un incremento del 164% rispetto ai primi sei mesi del 2016.[2]

Ad ogni nuova violazione aumenta la preoccupazione che la privacy dei dati sia ormai completamente compromessa. Secondo un recente studio, le persone sentono che la loro privacy è sottoposta ad attacchi alla sicurezza e alla riservatezza. In effetti, il 91 percento ha paura che le persone non abbiano completa conoscenza di come i propri dati personali vengano raccolti ed utilizzati dalle aziende. Un numero pressoché uguale di persone crede che sarebbe molto difficile rimuovere informazioni inesatte che le riguardano online.[3] Non sono solo le gravi violazioni a destare preoccupazioni. Il fatto che le piccole imprese abbiano un minor numero di informazioni su una persona non significa che il furto o l'uso improprio di esse sia meno importante per la persona interessata.

Queste paure aumentano in continuazione anche se, da più di un decennio, sono in vigore direttive e normative sulla privacy e la protezione dei dati estremamente rigorose. La normativa HIPAA (Health Insurance Portability and Accountability Act), la legge Fair Credit Reporting Act negli USA e la Direttiva sulla protezione dei dati nella U.E. sono solo alcuni dei maggiori esempi.

La Direttiva sulla protezione dei dati delinea i principi, come ad esempio il requisito che i dati debbano essere conservati in modo sicuro, elaborati per scopi limitati e mantenuti per un periodo di tempo non superiore a quello necessario. Tuttavia, si tratta pur sempre di una "direttiva" e non di una legge, e la sua effettiva adozione e applicazione in ogni paese europeo varia.

Alla scoperta del GDPR

Il GDPR è il regolamento più completo e di più grande impatto a livello globale introdotto per proteggere i dati personali. Il GDPR è stato creato a causa del principio condiviso che ogni persona abbia il diritto fondamentale alla privacy. L'obiettivo è proteggere la privacy delle persone nell'UE mediante l'applicazione di un nuovo regolamento sul modo in cui le aziende custodiscono, elaborano e utilizzano i dati personali.

Il GDPR può essere il passo in avanti più significativo degli ultimi vent'anni in materia di protezione dei dati e della privacy, sia per i requisiti di responsabilizzazione (accountability) relativi al trattamento dei dati, che per il suo potenziale impatto economico-finanziario. Il regolamento prevede due livelli di sanzioni: le organizzazioni possono essere penalizzate per un importo pari al 2 percento del fatturato globale annuo o a €10 milioni per violazioni come:

- Omissione di notifica a una autorità di vigilanza e alle persone interessate da una violazione dei dati
- Mancanza della nomina di un funzionario responsabile della protezione dei dati (DPO) se il tipo di organizzazione ne richiede uno

Le organizzazioni possono essere soggette a una multa del 4 per cento del fatturato globale annuo/€20 milioni per violazioni come:

- Non osservanza dei diritti degli interessati
- Violazione di un ordine di un'autorità di vigilanza
- Violazione dell'obbligo di conformarsi ai requisiti per il trasferimento internazionale dei dati[4]

Tali sanzioni si aggiungono alla perdita di reputazione, alla riduzione del valore e della fiducia nel marchio - che possono essere altrettanto devastanti per i profitti dell'azienda. Infatti, la pubblicizzazione dei casi di violazione dei dati, nel 65 per cento delle persone, provoca la perdita di fiducia nell'organizzazione che l'ha subita.[5]

La conformità GDPR non è un adempimento da prendere alla leggera, in quanto le organizzazioni sono responsabili delle modalità di raccolta, utilizzo, gestione ed eliminazione dei dati personali, il tutto preservando la sicurezza dei dati. Anche le organizzazioni che già hanno adottato programmi per la

Il GDPR è il regolamento più completo e di maggiore impatto introdotto a livello globale per proteggere i dati personali.[1]

privacy e la sicurezza dovranno rivalutare le loro procedure. Specificamente, il GDPR richiede alle organizzazioni di implementare appropriate misure tecniche e organizzative per impedire la perdita o l'accesso non autorizzato ai dati personali.

Questo genera ulteriori quesiti, come:

D. Cosa s'intende con dati personali?
R. Qualsiasi informazione relativa a una persona fisica identificata o identificabile.[6] Questo potrebbe includere i dati identificativi (come ad esempio un nome o un numero identificativo) o dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, le informazioni sulla salute, i reati penali, le previsioni sul rendimento lavorativo, la situazione economica, le preferenze o gli interessi personali, l'affidabilità o il comportamento, la posizione o i movimenti, ecc.[7]

D. Cosa è la pseudonimizzazione, e perché dovrebbe interessarmi?
R. Il termine "pseudonimizzazione", citato 15 volte nel GDPR, indica una procedura in base alla quale i campi con dati identificabili di un record di dati vengono sostituiti da uno o più identificatori artificiali, o pseudonimi. Il GDPR raccomanda l'applicazione della pseudonimizzazione ai dati personali per ridurre i rischi per i soggetti ai quali si riferiscono i dati e per aiutare gli addetti al controllo e al trattamento dei dati a soddisfare i loro obblighi di protezione.[8]

D. Le organizzazioni possono ottenere il consenso delle persone per raccogliere i loro dati personali?
R. Sì, ma il consenso deve essere concesso in base a informazioni indicanti in modo chiaro e risoluto che le informazioni vengono concesse in modo libero, specifico, informato e con inequivocabile consenso della persona interessata al trattamento dei dati personali. Le caselle pre-selezionate, il tacito assenso o l'inattività non costituiscono consenso.[9] Le organizzazioni devono mantenere la documentazione della concessione del consenso e assicurarsi che tali richieste di consenso siano distinguibili da altre richieste, utilizzando un linguaggio chiaro e comprensibile.[10] L'Articolo 13 delinea le ampie informazioni che devono essere fornite al soggetto interessato al momento della raccolta dei dati personali, come ad esempio lo scopo della raccolta delle informazioni, i destinatari o le categorie di destinatari dei dati personali e il periodo di tempo di memorizzazione dei dati.

D. Che cosa è la Data Protection Impact Assessment (DPIA)?
R. Una DPIA, ovvero la valutazione d'impatto in caso di violazione, è una valutazione richiesta per attività ad alto rischio che aiuta le organizzazioni a valutare l'origine, la natura, la particolarità e la gravità dei rischi e ad attuare le misure appropriate per ridurre tali rischi, come ad esempio mediante crittografia. Nel valutare i rischi per la sicurezza dei dati, occorre prendere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione, la perdita o l'alterazione accidentale o illecita, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, memorizzati o altrimenti elaborati che possono portare a danni fisici, materiali o immateriali.[11]

D. Devo nominare un funzionario responsabile della protezione dei dati (DPO)?
R. La designazione di un DPO è obbligatoria ogniqualvolta l'elaborazione dei dati venga effettuata da un ente pubblico (tranne i tribunali che agiscono esercitando la propria capacità giudiziaria) o per una società le cui attività principali consistono in operazioni di elaborazione che richiedono il monitoraggio regolare e sistematico dei dati dell'interessato su larga scala. La nomina di un DPO è obbligatoria anche per tutte le imprese che elaborano su larga scala dati contenenti informazioni sensibili, come ad esempio dati sulla salute, le convinzioni religiose o politiche. Specificamente, il DPO...

- Deve essere nominato sulla base delle qualità professionali e in particolare per la competenza sulle normative e le procedure relative alla protezione dei dati
- Può essere un membro del personale o un fornitore di servizi esterno
- I suoi dati dovranno essere forniti all'Autorità competente sulla protezione dei dati (DPA)
- Deve essere dotato di risorse adeguate per svolgere il proprio compito e mantenere la propria competenza aggiornata
- Deve far capo direttamente ai più alti livelli del management
- Non deve effettuare qualsiasi altra attività che potrebbe causare un conflitto di interesse.[12]

Sicurezza fisica e requisiti di privacy
Che cosa devono fare le organizzazioni per prevenire le violazioni dei dati? L'Articolo 24 del GDPR delinea la responsabilità di un'organizzazione nell'attuazione di "appropriate misure tecniche e organizzative" per garantire e dimostrare il corretto trattamento dei dati personali. L'Articolo 32 compie un ulteriore passo in avanti spiegando che "nel valutare il livello di protezione appropriato, si dovrà tener conto dei rischi che sono presentati dall'elaborazione, e in particolare, dalla distruzione, perdita, alterazione accidentale o illecita, dalla divulgazione non autorizzata o dall'accesso a dati personali trasmessi, memorizzati o altrimenti elaborati."

Un aspetto importante di questo regolamento è l'enfasi sulla prevenzione degli accessi non autorizzati. Sotto questo aspetto la sicurezza fisica è essenziale. In particolare, si possono proteggere i dati contro le minacce umane interne ed esterne che mirano a sfruttare eventuali lacune all'interno delle strutture fisiche dell'organizzazione o dei suoi dipendenti. Queste operazioni includono la limitazione dei dati che possono essere osservati, sottratti od ottenuti. Esaminare quanto segue e valutare se i dipendenti dell'organizzazione abbiano adottato le appropriate misure tecniche ed organizzative per ottenere la conformità.

Implementazione della protezione dei dati "by design" e "by default":
Proteggere i dati "by default" significa che le organizzazioni devono identificare e raccogliere in modo proattivo solo i dati personali necessari per gli scopi specificati, conservare i dati solo per il tempo necessario (principio di minimizzazione) e garantire che i dati personali non siano resi accessibili a un numero indefinito di persone. Probabilmente le organizzazioni dovranno accertarsi che i rischi relativi alla privacy siano identificati prima e che i sistemi siano progettati per attenuare tali rischi, mediante l'appropriata pseudonimizzazione e anonimizzazione, un approccio trasparente alle funzioni di trattamento dei dati e l'identificazione delle persone o dei ruoli specifici che devono accedere ai dati. Chiedetevi: Avete preso in considerazione i rischi relativi alla privacy degli interessati prima di progettare i sistemi informatici, le procedure commerciali e le strutture fisiche? Avete incontrato il vostro personale IT per esaminare gli attuali sistemi e le attività di elaborazione e per discutere se sono necessarie ulteriori operazioni per documentare in che modo i dati personali saranno protetti durante tutto il ciclo di vita dei dati?

Utilizzo di protezioni fisiche:
Per quanto i controlli di sicurezza informatica, come ad esempio la crittografia dei dati e le password complesse, siano elementi particolarmente critici, anche i controlli amministrativi e fisici a basso contenuto tecnologico sono ugualmente importanti. Per determinare dove siano necessarie barriere fisiche, è necessario identificare i punti di accesso alle informazioni sensibili. Per esempio, spesso i dipendenti utilizzano dispositivi mobili per accedere e condividere i dati da qualsiasi luogo. Un numero crescente di questi lavoratori ha bisogno di accedere alle informazioni sensibili in luoghi pubblici, spesso esposti alla vista di altri. Anche il rischio di esposizione dei dati all'interno degli uffici è aumentato. La normale disposizione open-space degli spazi aziendali rimuove le barriere fisiche che tradizionalmente contribuivano a proteggere gli schermi di computer. Chiedetevi: avete posizionato gli schermi dei computer lontano da porte e finestre e dalle aree accessibili al pubblico? Avete dotato i monitor e i dispositivi mobili di schermi per la privacy per oscurare la visualizzazione delle informazioni a potenziali occhi indiscreti? Le stampanti/copiatrici/fax condivise si trovano in aree protette o hanno coperchi bloccabili? Archiviate le copie cartacee dei dati in una struttura che prevede il controllo degli accessi? I tritadocumenti sono disponibili come dotazione standard nelle apposite aree, specialmente nei pressi di fotocopiatrici, stampanti e fax e sono un prerequisito per tutti coloro che lavorano a distanza o utilizzano connessioni remote per accedere alle informazioni aziendali?

Programmi di formazione dei dipendenti:
I programmi di formazione dovrebbero soddisfare tre aspetti chiave: Le migliori prassi in termini di osservazione, accesso fisico e prevenzione di furti. Per esempio, sarà necessario ricordare ai dipendenti di vigilare su ciò che li circonda nei luoghi pubblici quando operano accedendo a dispositivi collegati tramite i loro computer portatili, tablet e smartphone. Le schermate dei dispositivi non dovrebbero essere esposte alla vista di passanti e potenziali sguardi indiscreti, specialmente quando si inseriscono dati di accesso o si visualizzano informazioni sensibili sul proprio account. In situazioni di accesso fisico, le organizzazioni dovrebbero fornire ai propri dipendenti una formazione adeguata su come eliminare le informazioni dalle lavagne bianche e raccogliere documenti riservati al termine delle riunioni, memorizzare le password invece di trascriverle, chiudere a chiave gli schedari e i computer portatili, utilizzare filtri per la privacy sui dispositivi informatici e osservare la metodologia "clean desk policy" (CDP) per mantenere le scrivanie pulite e libere ed uscire/disconnettersi dai dispositivi prima di lasciarli non presidiati. Chiedetevi: Il vostro programma di formazione comprende la consapevolezza situazionale che consente ai dipendenti di acquisire una conoscenza del loro ambiente, necessaria a identificare e rispondere ai comportamenti sospetti? I dipendenti si rendono conto delle aspettative dell'organizzazione per quanto riguarda la metodologia CDP? Vi capita spesso di ricordare ai dipendenti le migliori prassi che dovrebbero osservare per la sicurezza?

Sviluppo di politiche chiare:
Per dimostrare l'impegno di un'organizzazione nell'attuazione di opportune misure di sicurezza e di privacy, le politiche dovrebbero definire che cosa i dipendenti e i collaboratori dovrebbero fare e non fare in termini di visualizzazione e utilizzo delle informazioni, sia nel normale ambiente lavorativo che in modalità remota. Gli accordi dei dipendenti dovrebbero contenere espressioni specifiche sulla responsabilità di salvaguardare informazioni sensibili e riservate.[13] Chiedetevi: Avete comunicato chiaramente alle persone i vostri intendimenti sulla salvaguardia della privacy e della sicurezza, spiegando come l'organizzazione debba proteggere, condividere, eliminare e permettere l'accesso ai dati personali? L'organizzazione ha adottato una politica BYOD (Bring Your Own Device) per gestire i comportamenti dei dipendenti e i necessari controlli di sicurezza anche quando accedono alle risorse aziendali dai loro dispositivi personali? Nell'ambito di tale politica di sicurezza, avete stabilito che i dipendenti dovrebbero utilizzare controlli di sicurezza sia visivi che informatici?

Impostazione dei limiti per la memorizzazione dei dati:
Le organizzazioni dovrebbero definire i periodi di tempo di memorizzazione dei dati personali in conformità con le normative vigenti. Tutti i dati personali che non sono assolutamente necessari a supportare i fini commerciali per i quali sono stati acquisiti dovrebbero essere eliminati in modo sicuro. Chiedetevi: Quali controlli tecnici

sono stati adottati per eliminare i dati al momento giusto? Le procedure di eliminazione e distruzione della vostra organizzazione soddisfano le rigorose linee guida di sicurezza, come, ad esempio, quelle indicate nella Guida speciale NIST 800-88 per la distruzione fisica delle unità di memoria che hanno superato i termini di vita utile?

Verifica dei fornitori esterni:
Accertatevi che gli operatori e/o il personale preposto al trattamento dei dati consenta sufficienti garanzie in termini di conoscenza specifica, affidabilità e risorse per implementare misure tecniche e organizzative, compresa la sicurezza dei dati durante il trattamento. Chiedetevi: L'organizzazione ha adottato un programma di gestione dei fornitori che includa gli obblighi contrattuali e stabilisca attività di verifica da parte del management per i fornitori e le persone che hanno accesso ai dati personali?

Creazione di un protocollo di violazione dei dati:
Quando vengono a conoscenza del fatto che si è verificata una violazione dei dati personali, le organizzazioni dovranno essere preparate a informare l'autorità di vigilanza senza indebito ritardo (se possibile, non più tardi di 72 ore). Oppure essere in grado di dimostrare che è improbabile che la violazione dei dati personali possa comportare un rischio per la tutela dei diritti e delle libertà delle persone fisiche. In caso di rischio elevato, sarà necessario informare anche le persone interessate dalla violazione dei dati senza indebito ritardo.[14] Chiedetevi: Quando è stata effettuata l'ultima revisione delle politiche e dei piani di risposta agli incidenti e di notifica delle violazioni dell'organizzazione? I dipendenti saprebbero chi informare all'interno dell'organizzazione nel caso in cui il loro dispositivo fosse compromesso o se venissero a conoscenza di una violazione dei dati? L'organizzazione ha implementato un piano di risposta in caso di incidenti e di notifica delle violazioni per determinare quando e come notificare tali eventuali violazioni dei dati alle autorità?

Conoscere i diritti delle persone interessate:
Ora i cittadini residenti nell'UE hanno il diritto di vedere quali dati personali le organizzazioni detengono su di loro, e in alcuni casi chiedere che i loro dati vengano eliminati. Il diritto all'eliminazione dei record prevede che le organizzazioni eliminino qualsiasi link o copia o replica di tali dati personali. Le organizzazioni dovrebbero fornire una procedura che garantisca alle persone di inoltrare tali richieste in forma elettronica, specialmente se i dati personali sono trattati con mezzi elettronici.[15] Chiedetevi: La vostra organizzazione è consapevole di cosa s'intenda con "dati personali" e di come rispondere a eventuali richieste riguardanti i dati personali?

Conclusione:

Il regolamento GDPR rappresenta la più significativa evoluzione normativa degli ultimi vent'anni sulla privacy dei dati. Richiede la gestione dei dati personali in modo da garantire un'adeguata sicurezza e riservatezza, un compito che comporta l'adozione di misure di sicurezza sia tecniche che organizzative. Inoltre, le sanzioni previste per la mancata conformità potrebbero essere paralizzanti per le organizzazioni. D'altro canto le migliori prassi descritte nel regolamento rappresentano semplicemente delle buone procedure commerciali. Nessun individuo desidera che le proprie informazioni vengano utilizzate in modo improprio, e nessuna organizzazione desidera affrontare le conseguenze di una violazione dei dati. Le organizzazioni che intendono la privacy non come un mero adempimento giuridico ma come una responsabilità aziendale possono utilizzarla come vantaggio strategico per migliorare la loro reputazione e il valore del marchio, attirare talenti e consolidare la fiducia del pubblico.

www.3mitalia.it/privacy-protezione

[1]Forrester, Lessons Learned from the World's Biggest Security Breaches and Data Abuses, 9 gennaio 2017
[2]2017 Gemalto Breach Level Index, http://www.gemalto.com/press/Pages/First-Half-2017-Breach-Level-Index-Report-Identity-Theft-and-Poor-Internal-Security-Practices-Take-a-Toll.aspx
[3]GfK Privacy Panel, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014.
[4]Articolo 83, regolamento GDPR, 2017
[5]Ponemon Institute, The Impact of Data Breaches on Reputation & Shared Value, Sponsorizzato da Centrify, 2017.
[6]Articolo 4, regolamento GDPR, 2017
[7]Premessa 75, regolamento GDPR, 2017
[8]Premesse 26 e 28, regolamento GDPR, 2017
[9]Premessa 32, regolamento GDPR, 2017
[10]Articolo 7, regolamento GDPR, 2017
[11]Articolo 35 e Premesse 83-84, regolamento GDPR, 2017
[12]Articoli 37-38, regolamento GDPR, 2017
[13]Premesse 74, 77 e 78, regolamento GDPR, 2017
[14]Premessa 81, regolamento GDPR, 2017
[15]Premesse 59, 63, 65 e 66, regolamento GDPR, 2017

The experts in screen privacy. | 3M