DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

The British Chamber of Commerce for Italy

I PRINCIPI CHIAVE DEL REGOLAMENTO; I NUOVI DIRITTI DEGLI INTERESSATI E GLI OBBLIGHI DI DOCUMENTAZIONE E NOTIFICAZIONE IN CAPO ALLE AZIENDE. RESPONSABILI E RESPONSABILITÀ

Bridget Ellison, Studio De Berti Jacchia Franchini Forlani

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

ALCUNI ASPETTI CHIAVE DESTINATI AD AVERE GRANDE IMPATTO SULL'OPERATIVITÀ DELLE IMPRESE

Saranno affrontati i seguenti temi chiave:

- Accountability del titolare e del responsabile del trattamento
- Privacy by Design, Privacy by Default
- I nuovi diritti dell'interessato
- Il Responsabile per la Protezione dei Dati Personali (Data Privacy Officer)
- Caratteristiche nuove del Responsabile del Trattamento

ACCOUNTABILITY

Cosa significa accountability?

Responsabilizzazione dell'azienda con obbligo di rendiconto:

- dopo UN'ATTENTA VALUTAZIONE DEL RISCHIO nel proprio contesto operativo, l'impresa determina in autonomia, utilizzando gli strumenti indicati dal Regolamento, e mette in atto
- le misure tecniche ed organizzative ADEGUATE al rischio per garantire ED ESSERE IN GRADO DI DIMOSTRARE, che il trattamento garantisce la protezione dei dati personali conformemente al Regolamento

IMPATTO: NECESSITÀ DI CREARE UNA TRACCIA INFORMATICA O CARTACEA

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

STRUMENTI PER DIMOSTRARE LA CONFORMITÀ

Quali sono gli strumenti per dimostrare che l'impresa abbia messo in atto le misure tecniche ed organizzative adeguate per garantire la privacy?

- Registro delle attività di trattamento
- Protocolli, procedure
- Adesione a codici di condotta (redatte dalle associazioni di categoria)
- Certificazione da organismi riconosciuti
- Valutazione d'impatto sulla protezione dei dati personali

PRIVACY BY DESIGN – PRIVACY BY DEFAULT

Privacy by Design = la protezione della privacy e la sicurezza dei dati personali devono essere integrati fin dalla progettazione nei sistemi informatici e gestionali dell'azienda

Privacy by default = in assenza di qualsiasi atto positivo vengono trattati solo i dati personali necessari per la finalità autorizzata

Le misure tecniche ed organizzative determinate dall'impresa dovranno quindi essere:

- integrate in un sistema strutturale (Data Protection Management System)(Modello di Gestione dei Dati Personali) che preveda anche un monitoraggio costante, e
- progettato in maniera tale da garantire la protezione dei dati

IMPATTO: ISTITUZIONE DI UN MODELLO DI GESTIONE DEI DATI PERSONALI

I NUOVI DIRITTI DELL'INTERESSATO…

CODICE PRIVACY	REGOLAMENTO
indicazione origine, finalità e logica del trattamento	**Diritto alla portabilità dei dati (accesso, copia in formato strutturato e leggibile per trasferimento ad altri titolari)**
cancellazione dei dati SOLO se trattati in violazione della legge	**Diritto all'oblio (cancellazione se:** ▪ **i dati non sono necessari** ▪ **per la finalità** ▪ **se revocato il consenso)**

…E I NUOVI OBBLIGHI DEL TITOLARE

Comunicazione a terzi di cancellazione su richiesta dell'interessato

→ **Obbligo di notificare a tutti i destinatari dei dati**

Obbligo di notifica al Garante solo in determinati casi

→ **Obbligo di notificare data breach:**
- **al Garante - sempre**
- **all'interessato -**
- **elevato rischio**

IMPATTO: NECESSITA' DI ORGANIZZARE LE BANCHE DATI PER FAR FRONTE AI NUOVI DIRITTI E OBBLIGHI

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

RUOLO DEL DATA PROTECTION OFFICER

Qual è il ruolo del Responsabile per la Protezione dei Dati Personali?

- FUNZIONI: deve essere coinvolto in tutte le questioni che riguardino la protezione dei dati personali, informare e consigliare il titolare sul rispetto del Regolamento, sorvegliare l'osservanza del Regolamento e del Modello di Gestione dei Dati Personali, fungere da contatto con il Garante
- RUOLO: deve essere una figura esperta in materia di privacy e indipendente, che faccia riferimento direttamente ai vertici aziendali e che disponga delle risorse umane ed economiche per assolvere ai propri compiti
- Nomina obbligatoria solo: per enti pubblici, o in caso di trattamenti che richiedano monitoraggio regolare e sistematico degli interessati su larga scala o di dati sensibili e giudiziari su larga scala MA opportuna per ogni società con una struttura minimamente articolata

IMPATTO: NUOVO ORGANIGRAMMA PRIVACY

RESPONSABILE DEL TRATTAMENTO

Come cambia la figura del responsabile del trattamento?

- Responsabile “interno” a sensi dell’art 29 del Codice Privacy non è previsto dal Regolamento
- Il Responsabile del Trattamento è qualunque soggetto che effettui trattamenti di dati personali per conto del titolare del trattamento
- Tali trattamenti devono essere disciplinati da un CONTRATTO contenente specifici obblighi per la protezione dei dati personali in capo al Responsabile

Il Responsabile del trattamento è DIRETTAMENTE RESPONSABILE (solidalmente con il Titolare)

- Per il danno cagionato dal suo trattamento in violazione delle norme o se non ha seguito le istruzioni del Titolare
- Per le sanzioni relative

IMPATTO: NUOVI RAPPORTI TITOLARE/RESPONSABILE

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

… PER CONCLUDERE…

- Accountability ➡ Il titolare dovrà poter rendere conto della propria gestione dei dati personali, creando una traccia documentale
- Privacy by Design e Privacy by Default ➡ Modello di Gestione per garantire la protezione dei dati personali, minimizzandone il trattamento per impostazione predefinita
- Nuovi diritti e nuovi obblighi ➡ L'impresa dovrà ristrutturare le proprie banche dati
- DPO ➡ Nuovo organigramma privacy
- Responsabile del trattamento ➡ Cambia la dinamica del rapporto e la divisione di responsabilità con il titolare

BRIDGET ELLISON

b.ellison@dejalex.com
www.dejalex.com

20121 Milano
Via San Paolo 7
Tel. +39 02 72554.1
Fax +39 02 72554.600

20121 **MILANO**
Via San Paolo, 7
tel. +39 02 72554.1
fax +39 02 72554.500

milan@dejalex.com

00198 **ROMA**
Via Vincenzo Bellini, 24
tel. +39 06 809154.1
fax +39 06 809154.44

rome@dejalex.com

1170 **BRUXELLES**
Chaussée de La Hulpe 187
tel. +32 (0)2 645 5670
fax +32 (0)2 742 0138

brussels@dejalex.com

115114 **MOSCA**
Ulitsa Letnikovskaya, 10
tel. +7 495 792 54 92
fax +7 495 792 54 93

moscow@dejalex.com

DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

The British Chamber of Commerce for Italy

RISK ASSESSMENT E VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI. MISURE DI SICUREZZA

Giovanni D'Adamo, Development Compliance Partners

Sicurezza del trattamento

Articolo 32 – C83

Titolare o Responsabile del trattamento

<u>Valutazione dei rischi inerenti al trattamento</u>

- *Distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati*
- *<u>Pregiudizi derivati</u>: danni fisici, materiali o immateriali.*

<u>Attuazione di misure per limitare tali rischi</u>

Misure di sicurezza adeguate?

I parametri a monte della individuazione delle misure di sicurezza sono:

- *Stato dell'arte*

Costi di attuazione

Natura, oggetto, contesto e finalità del trattamento

Rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

Il Regolamento:

- **non** prevede un elenco di misure di sicurezza.
- esemplifica le misure adeguate da adottare a seconda dei risultati dell'analisi dei rischi / valutazione d'impatto.

Misure di sicurezza adeguate?

Tecniche

- **Pseudonimizzazione** e la cifratura dei dati personali
- Capacità di **assicurare su base permanente** la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- Capacità di **ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico
- Minimizzazione dei dati e dei trattamenti
- Definizione del periodo di conservazione
- Accessibilità dei dati

} Art. 25

Organizzative

- Distribuzione di responsabilità tra titolare e responsabile
- Designazione DPO
- Policy, linee guida, …procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento
- Formazione
- Adesione a **codici di condotta** o a un **meccanismo di certificazione** approvato

Misure espressamente previste dall'Art. 32

Guida del Garante al GDPR del 28.4.2017

- *La **lista è aperta e non esaustiva**.*
- ***Non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.*
- *Facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, **l'Autorità potrà valutare la definizione di linee-guida o buone prassi**.*
- ***Per alcune tipologie di trattamenti** (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) **potranno restare in vigore le misure di sicurezza attualmente previste** attraverso le disposizioni di legge volta per volta applicabili (es. trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico).*

Valutazione d'impatto

Articoli 35 e 36 – C84, C89-C93, C95

Quando?

In **generale**: uso di nuove tecnologie o rischio elevato per i diritti e le libertà delle persone fisiche

In **particolare**:

a)

- **Valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, basata su un **trattamento automatizzato**, compresa la **profilazione**, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche

b)

- Trattamento, su **larga scala**, di **categorie particolari di dati personali** o di dati relativi a **condanne penali e a reati**

c)

- **Sorveglianza sistematica su larga scala** di una zona **accessibile al pubblico**

Il Titolare del trattamento si **consulta con il DPO**, qualora designato.

Considerando 90: occorre valutare la particolare **probabilità** e **gravità** del rischio.

Valutazione d'impatto

Articoli 35 e 36 – C84, C89-C93, C95

La valutazione d'impatto sulla protezione dei dati deve contenere almeno:

Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento (e l'interesse legittimo perseguito dal Titolare del trattamento)

Una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità

a)Una valutazione dei rischi per i diritti e le libertà degli interessati

a)Le misure previste per affrontare i rischi

b)(garanzie, misure di sicurezza e meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento)

Valutazione d'impatto

Articoli 35 e 36 – C84, C89-C93, C95

*Se dalla valutazione d'impatto emerge che il rischio per la protezione dei dati **non** potesse essere ragionevolmente attenuato mediante l'uso delle tecnologie disponibili e per gli elevati costi di attuazione, è opportuno **consultare l'autorità di controllo** prima dell'inizio delle attività di trattamento.*

*Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati **almeno quando insorgono variazioni del rischio** rappresentato dalle attività relative al trattamento.*

Minacce tecnologiche e Cyber Security

Il Cyber Crime nel 2016

Fonte: Rapporto Clusit 2017 sulla Sicurezza ICT in Italia

Nel 2016 sono stati registrati 1.050 attacchi considerevoli
(+3,75% rispetto al 2015)

Numero di attacchi informatici in Italia per tipologia e variazione sul 2015:

Motivazioni:	***Metodi:***	***Settori più colpiti***
• Cybercrime 751 (+9,8%)	• Phishing +1.166%	• Sanità +102%
• Hacktivism 161 (-23,00%)	• Malware + 116%	• Grande distribuzione + 116%
• Spionaggio/sabotaggio 88 (+8,3%)		• Banche e finanziarie +64%
• Guerra cibernetica 55 (+117,4%)		

Cyber attacks

Fonte: Rapporto Banca d'Italia 2017

Le principali evidenze:

- 1,5% delle imprese italiane non adotta alcuna misura difensiva
- 30,3% delle imprese dichiara di aver subito danni a causa di un attacco informatico tra settembre 2015 e settembre 2016
- I tassi di attacco si sono rivelati più bassi per le imprese con sede nel Sud Italia (39,5%)
- I tassi di attacco più alti (62,8%) riguardano le aziende con più di 500 dipendenti
- Le più colpite sono le imprese di maggiori dimensioni, quelle con elevato contenuto tecnologico e quelle esposte sui mercati internazionali, perché tendono a gestire un numero maggiore di dati di valore.

Cyber Crime

- I criminali hanno capito rapidamente come sfruttare la velocità, la convenienza e l'anonimato garantiti da Internet per svolgere attività illegali
  - Spam & Phishing
  - Frodi
  - Furto di Dati
  - Estorsione
  - Attacchi Informatici
  - Black Market

Phishing – Come funziona?

- Via email:
  - Si riceve un’email fittizia che si spaccia per legittima
  - Spesso provengono da indirizzi molto simili a quelli originali
    - (i.e. admin@lamiabnca.it invece che admin@lamiabanca.it)
- Via chat:
  - Link a siti farlocchi, molto simili ad altri siti noti, ma su domini diversi
    - (i.e. labanca.sicuro.it invece che sicuro.labanca.it)
- In entrambi i casi, verranno richieste informazioni private
  - Credenziali di accesso
  - Dati anagrafici
  - Dati di pagamento (es. carte di credito)

Phishing Scenario #1

1

da: **info@banca.it**

email di Social Engineering con indirizzo modificato

2

finta email della banca della vittima con **link** a un sito malevolo

la vittima clicca sul link **http://banca.ru**

3

banca.ru
(si finge il sito banca.it)

4

richiesta dati di pagamento per evitare il blocco della carta

5 sottrazione di denaro

Phishing Scenario #2

1

da: **info@banca.it**

email di Social Engineering con indirizzo modificato

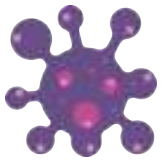
2

finta email della banca della vittima con **allegato**

3 la vittima apre l'allegato

«modulo.**docx** .exe»
il file è in realtà un eseguibile!

4 il file contiene un **malware** per prendere il controllo del PC



5 il PC viene utilizzato per attività illecite

[redacted] sei sotto inchiesta

Da: Procura della Repubblica (eugen.taranu@cosmef.it)

A: [redacted]

Procuratore della Repubblica
presso il Tribunale ordinario

INVIATA PER LA PRESENTAZIONE
DI PERSONA SOTTOPOSTA AD INDAGINI

-art. 375 c.p.p.-

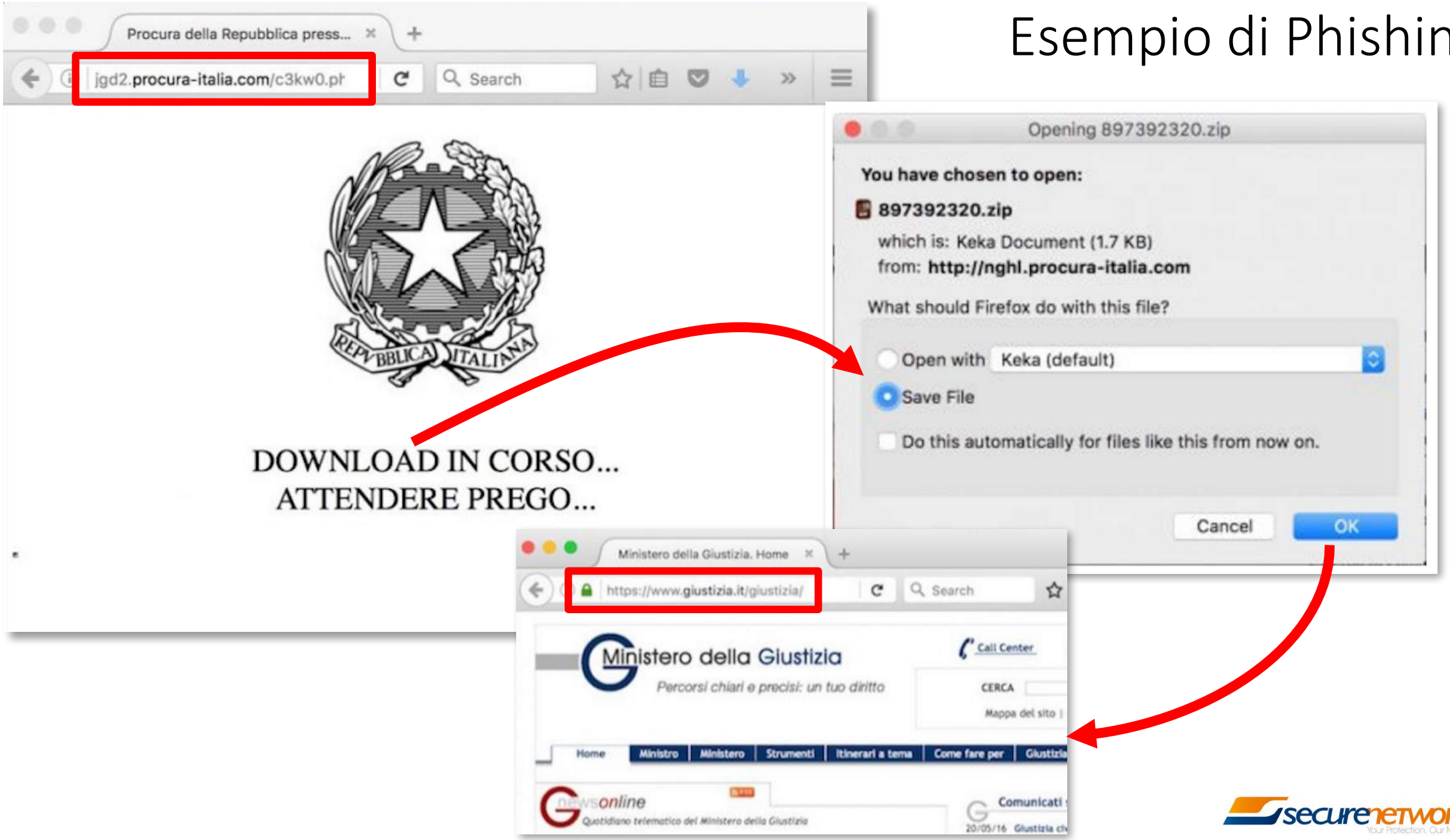
La presente per comunicarLe che il Suo patrimonio immobiliare, così come il Suo conto corrente bancario, verranno posti in arresto con l'accusa di mancato pagamento delle imposte e concorso in riciclaggio di denaro, ad effetto della causa 61802503
L'arresto entra in vigore dal 27.05.16
Lei potrà prendere visione della causa 61802503 cliccando sul link
In questo documento Lei ha la possibilità di trovare informazioni su come ricorrere in appello, il nominativo del giudice inquirente per la causa che La riguarda, la data e il luogo del dibattimento.
Nel caso in cui Lei non si presentasse al dibattimento, lo stesso avrà luogo anche in Sua assenza.
In caso di sentenza di condanna, Le verrà confiscata ogni proprietà e rischia una condanna fino a 15 anni di reclusione.

Esempio di Phishing

- L'indirizzo email sorgente non usa il dominio ufficiale
- Danno del "Lei", ma non usano mai il nome dell'utente
- Provano a convincerci a cliccare un link
- Come fa la Procura a conoscere la vostra email personale / aziendale?
- Comunicazioni importanti e giudiziarie sarebbero inviate tramite raccomandata o PEC

securenetwork
Your Protection, Our Mission

Esempio di Phishing



Malware = Soft***ware mal***evolo

- Cosa fa:
  - Interrompe o danneggia un sistema.
  - Colleziona informazioni sensibili.
  - Prende controllo di un sistema informatico o parte di esso.
- Perché lo fa:
  - Proof of concept – Dimostrazione dell'esistenza di un problema.
  - Guadagno economico
    - Interesse diretto – Es. prendere controllo di account bancari.
    - Su commissione – Vendita di dati sensibili.
    - Indiretto – Arrecare danno ai concorrenti.
- Come lo fa:
  - Cercando di non farsi scoprire.

Ransomware

- Il ransomware ha come scopo convincere le vittime a **pagare un riscatto** (*ransom*) tramite minacce

- Il pagamento viene richiesto tramite **modalità non tracciabili** (e.g. Bitcoin, Western Union) per mantenere l'anonimato

- Le versioni più comuni **impediscono l'accesso** alla postazione di lavoro o a determinati file / cartelle

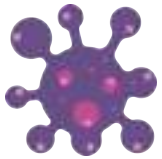
- Una delle varianti più diffuse è senz'altro **cryptolocker**, sviluppato per cifrare tutti i dati ai quali riesce ad accedere

Cryptolocker Scenario

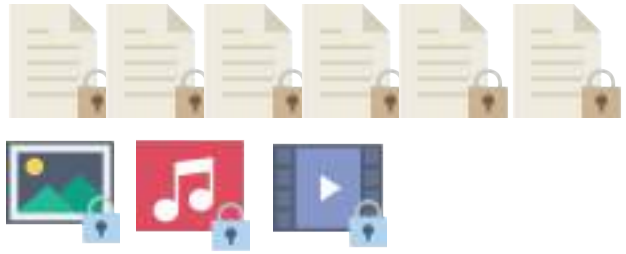
1 un dipendente riceve un'email con un **allegato**

2 la vittima **apre ed esegue** l'allegato

3 il file contiene un **malware** che infetta il computer



4 il **ransomware** cifra tutti i file che trova sul computer



5 il **ransomware** non si ferma ai soli dischi locali

6 il malware accede a **tutti i dischi possibili**

7 anche i contenuti delle **cartelle di rete aziendali** sono cifrati

securenetwork
Your Protection, Our Mission

Aprendo il File Scaricato…

Richiesta di Riscatto

(on)Top secret code?

securenetwork
Your Protection, Our Mission

Casi mediatici – Super Bowl Americano

Casi mediatici – RAF e Principe William

- **LinkedIN,** azienda statunitense, è uno dei principali Social Network;
- Nel 2012 ha subito un data breach che ha avuto come conseguenza il furto e il conseguente leak di 167 Milioni di credenziali;

- **YAHOO,** azienda statunitense, è uno dei principali Motori di Ricerca;
- Nel 2013 ha subito un data breach che ha avuto come conseguenza il furto e il conseguente leak di 1 Billion di credenziali;
- Solo nel 2016 l'azienda ha dato notizia delbreach a seguito di un leak;

Conclusioni: conoscere per prevenire

Vi sono due principali metodi per difendersi:

- **Formazione**: conoscere il fenomeno e i sui metodi resta il miglior modo per difendersi

- **Simulazione di attacchi:** analizzare periodicamente sistemi ed applicazioni, creare false *campagne di phishing* per addestrare i dipendenti dell'azienda e analizzare by Design anche gli aspetti di security dei nuovi prodotti IoT pensando a come gestire il monitoraggio e l'aggiornamento

Project steps

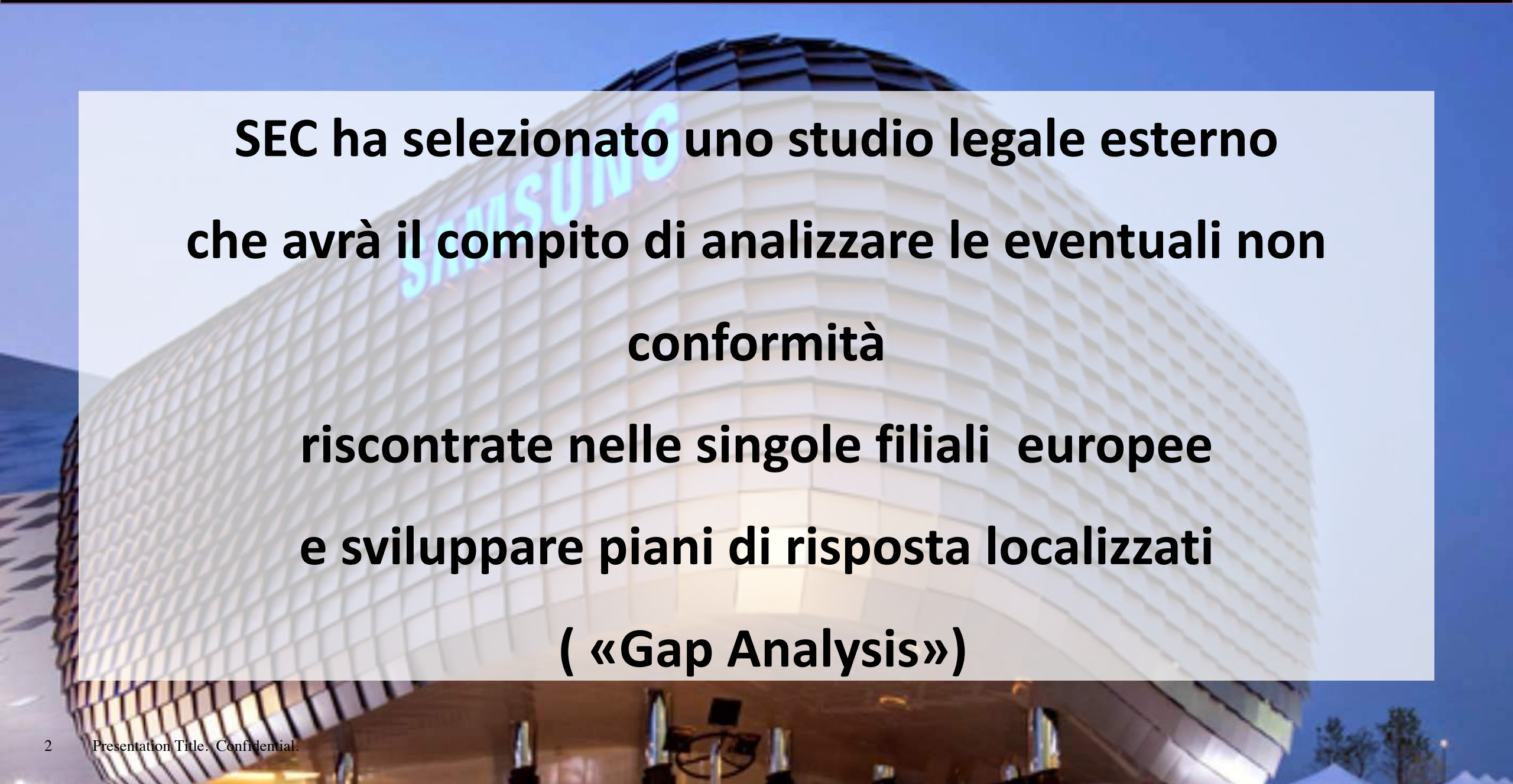
securenetwork
Your Protection, Our Mission

General Data Protection Regulation Project

Avv. Anna Rosetti
Legal Counsel
Samsung Electronics Italia S.p.A.

Milano, 22 Giugno 2017

Samsung Electronics Corea - HQ



SEC ha selezionato uno studio legale esterno

che avrà il compito di analizzare le eventuali non conformità

riscontrate nelle singole filiali europee

e sviluppare piani di risposta localizzati

(«Gap Analysis»)

STEP 1

Censimento di tutti i trattamenti effettuati nelle singole filiali Samsung raggruppandoli a seconda della finalità perseguita.

STEP 2

Analisi di ogni banca dati individuata,

secondo i parametri selezionati da SEC.

Per ogni singola banca dati devono essere indicate:

•le misure di sicurezza poste in essere per prevenire eventuali accessi non autorizzati

•se è stata fornita l'informativa privacy all'interessato

•se i dati vengono trasferiti fuori dall'UE

[…]

Samsung Electronics Italia

Al momento sono stati individuati n. 21 trattamenti e stiamo procedendo alla raccolta delle informazioni richieste da SEC.

Tale attività di «censimento» è stata agevolata dal fatto che SEI ha sempre mantenuto aggiornato il DPS.

Il termine, assegnato da SEC per la raccolta di tutte le informazioni, è la fine di giugno 2017.

Il «censimento» costituirà la base del Registro della attività di trattamento richiesto dal Regolamento UE.

L’Autorità Garante Privacy & SEI

A marzo 2010, l’ Autorità Garante Privacy ha avviato un procedimento nei confronti di SEI sulla base di una segnalazione da parte di un consumatore. Detto consumatore lamentava, che a seguito del malfunzionamento della propria stampante, aveva contattato il numero verde Samsung, messo a disposizione da SEI per finalità di assistenza alla clientela e, in tale occasione, il consumatore, in luogo dell’ informazione auspicata (vale a dire il riferimento del centro di assistenza più vicino), aveva ricevuto un messaggio che lo invitava a lasciare i suoi dati personali, in particolare il numero di telefono, ed il consenso al relativo trattamento.

L’Autorità Garante Privacy & SEI

A marzo 2016, l’ Autorità Garante Privacy, a fronte della segnalazione di un consumatore, ha chiesto dei chiarimenti a SEI circa la modalità di acquisizione del consenso per finalità promozionali e comunicazione dei dati personali tramite messaggio e-mail con pluralità di destinatari in chiaro.


THANKS

DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

The British Chamber of Commerce for Italy

TRASFERIMENTI DATI CROSS BORDER E *STATUS* INTESA EU - US

Giovanna Bagnardi, Studio De Berti Jacchia Franchini Forlani

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

RIFLESSIONI SUL (GDPR) NUOVO REGOLAMENTO

Trasferimento dati personali extra UE

Principio di adeguatezza

Valutazione di Adeguatezza

Standard Contractual Clauses

Binding Corporate Rules (BCR)

Trasferimenti Transfrontalieri /Autorità Capofila e *One-Stop-Shop*

Principio di collaborazione delle DPA

Status Privacy Shield

PRINCIPIO "*Adequate Level of Protection*"

Il Nuovo Regolamento (GDPR) conferma e riconosce il principio generale secondo il quale nel caso di trasferimenti dati personali extra UE

è necessario

" … *assicurarsi che i dati personali legalmente trattati e processati all'interno di EU e EEA rimangano (in ogni caso) soggetti a salvaguardia* … "

Pertanto, così come previsto anche dal Codice Privacy, rimangono vietati i flussi di dati extra UE, salvo che il paese importatore non sia in grado di garantire le tutele espresse nello stesso.

CP e (GDPR) NUOVO REGOLAMENTO (UE) 2016/679

Trasferimenti dati EXTRA UE ammessi

Valutazione di adeguatezza Commissione EU
(sul livello di protezione assicurato dallo Stato in questione)

In presenza di garanzie adeguate
(clausole standard di protezione; norme vincolanti d'impresa (BCR); Ricorrere di particolari situazioni

TRASFERIMENTI CROSS BORDER IN PRESENZA DI ADEGUATE GARANZIE (*Standard Contractual Clauses*)

Standard Contractual Clauses
(Clausole Contrattuali Tipo)

Commissione EU (già) promotrice di Clausole Contrattuali Standard
Attraverso 4 decisioni importanti per semplificare rapporti tra Stati

Controller To Controller
(Titolare vs Titolare)
+
Controller To Processor
(Titolare Vs Responsabile del T.)

Exporter / Importer
Exporter garantisce che i dati verranno trattati da Importer conformemente ai principi stabiliti nelle norme comunitarie

TRASFERIMENTI CROSS BORDER IN PRESENZA DI ADEGUATE GARANZIE (*Binding Corporate Rules- BCR*)

(BCR) Binding Corporate Rules
(Principi Vincolanti d'Impresa)

Clausole che stabiliscono principi vincolanti
che vincolano tutte
le società del medesimo
Gruppo d'impresa

[ES]: Principi di correttezza e legittimità del trattamento, finalità, necessità, proporzionalità dei dati, obbligo del titolare di fornire informazioni, etc.

[Approvazione BCR]
(approvate dalla DPA/Autorità di controllo competente o dall'Autorità capofila.
DPA deve darne comunicazione al Comitato ex art. 64.1f) al fine di ottenere il relativo parere. Commissione può specificare formato e procedure e scambio informazioni
tra T, R e DPA

TRASFERIMENTI CROSS BORDER IN PRESENZA DI ADEGUATE GARANZIE (*Binding Corporate Rules- BCR*)

(BCR) Binding Corporate Rules
(Principi Vincolanti d'Impresa)

[*Ratio*]
Trattandosi di rapporti continuativi tra diverse società e, quindi, tra diversi titolari e responsabili
È utile non dover sottoscrivere le clausole Standard / Tipo ogniqualvolta vi sia un trasferimento dalla controllante alla controllata o alle collegate

[art. 47.2 GDPR]
Fissa tutti i requisiti affinché BCR siano valide e consentano di prevedere una protezione adeguata nei flussi infra-gruppo.

(GDPR) NUOVO REGOLAMENTO E CONCETTO DI AUTORITÀ CAPOFILA (*Lead Authority*)

[art. 56 GDPR]
Introduce nuovo meccanismo
Autorità capofila
(*Lead Authority*)

Si attiva nel caso di cd.
"**Trattamento transfrontaliero**"

Trattamento dei dati ha luogo nell'ambito delle attività di stabilimenti in più di uno SM di un T o R del trattamento in UE se essi sono stabiliti in più di uno SM

Trattamento di dati ha luogo nell'ambito delle attività di un unico stabilimento di un T o R in UE qualora incida o probabilmente incida, in modo sostanziale, su interessati in più di uno SM

(GDPR) NUOVO REGOLAMENTO E CONCETTO DI AUTORITÀ CAPOFILA (*Lead Authority*)

Autorità Capofila
(*Lead Authority*)

Principio di Collaborazione
ai fini di certezza del diritto, omogeneità di soluzioni e approccio, facilitazione all'impresa, coerenza nell'applicazione del GDPR

Nei casi di "trattamenti transfrontalieri" descritti

DEVE essere individuata **Autorità di Controllo che funge da "capofila"** al fine di coordinare la **cooperazione** con le altre **autorità degli SM interessati**

- Autorità sarà quella dello SM dello "stabilimento principale" del T o del R oppure quella dello stabilimento unico del T o del R e ad essa dovrà rivolgersi p.es. l'autorità nazionale che ha ricevuto la segnalazione.
- Divieto Forum Shopping.

(GDPR) NUOVO REGOLAMENTO E CONCETTO DI AUTORITÀ CAPOFILA (*Lead Authority*)

In caso venga /debba essere adita l'Autorità Capofila
(*Lead Authority*)
per "trattamento transfrontaliero"

[art. 56 GDPR prevede
due possibili esiti]

art.56.4 Autorità di controllo capofila decide di trattare il caso
(meccanismo dello "**sportello unico**" o "***one-stop-shop***"
+ procedura ex art. 60)

Art. 56.5 Autorità di controllo capofila decide di NON trattare il caso
(DPA/autorità di controllo dello SM coinvolta (e che ha informato la capofila) dovrà farlo autonomamente nel rispetto degli artt. 61 e 62

DEROGHE AL MECCANISMO DELL'AUTORITA' CAPOFILA (*Lead Authority*)

[art. 56.2 GDPR]
DEROGA meccanismo
Autorità capofila
(*Lead Authority*)

Ogni DPA/Autorità di controllo di uno SM è competente per la gestione dei reclami ad essa proposti o per le violazioni del GDPR se l'oggetto
" …riguarda unicamente uno stabilimento nel suo SM o incide in modo sostanziale sugli interessati unicamente nel suo SM…"

In tal caso [art. 56.3 GDPR]
DPA/Autorità di controllo dello SM informa "senza indugio" l'Autorità capofila che entro 3 settimane decide se intende trattare il caso ex art. 60 ["sportello unico" /*one-stop-shop*], ovvero se DPA/Autorità di controllo dovrà trattare il caso a livello locale

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

STATUS PRIVACY SHIELD

[Caso Schrems C-362/15]
CGUE - 06.10.2015
dichiara invalida la decisione di adeguatezza relativa a US (Safe Harbour)

[Caso Schrems C-362/15]
Mr. Schrems (AU), utente Facebook dal 2008, denuncia presso local (IRL) DPA in quanto in seguito a rivelazione di Mr Snowden (2013) su NSA (National Security Agency US), diritto US non offre più tutela adeguata contro sorveglianza delle public authorities US su dati provenienti da altri paesi

DPA (IRL) respinge la richiesta sulla base dell'esistenza di decisione di adeguatezza espressa dalla Commissione. Mr Schrems si rivolge alla High Court of Ireland che, a sua volta, rinvia alla CGUE.

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

STATUS PRIVACY SHIELD

Accordo Privacy Shield
(transfer US/EU)
raggiunto 02.02.2016

Proposta/Progetto
"decisione di adeguatezza"
Commissione [29.02.2016]

WP 29 Parere su tale decisione [op.1/16],
in quanto sottoposta
alla procedura di Comitato
[ex art. 93 GDPR]
esprime critiche e perplessità

WP 29
- necessità di rivedere la Proposta alla luce dell'approvazione GDPR (aprile 2016)
- sulla base della decisione Schrems, accordo non rende un livello di protezione Equivalente, in particolare con riguardo a
(i) limiti conservazione dati;
(ii) limitazione delle finalità
(iii)difficoltà a far valere i propri diritti, etc.

STATUS PRIVACY SHIELD

WP 29 Parere (op 1/2016)
non vincolante

tuttavia, ha fatto **slittare adozione della decisione di adeguatezza Commissione al [12.07.2016]**

[06.04.2017] Parlamento EU invita la Commissione ad adottare misure necessarie per allineare Privacy Shield a GDPR

April 2017
WP 29 inizia discussione con Commissione per joint annual review of Privacy Shield (Sept 2017)

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

In attesa di ulteriori sviluppi
grazie per l'attenzione

Avv. Giovanna Bagnardi

Partner

g.bagnardi@dejalex.com
www.dejalex.com

20121 Milano
Via San Paolo 7
Tel. +39 02 72554.1
Fax +39 02 72554.600

20121 **MILANO**
Via San Paolo, 7
tel. +39 02 72554.1
fax +39 02 72554.500

milan@dejalex.com

00198 **ROMA**
Via Vincenzo Bellini, 24
tel. +39 06 809154.1
fax +39 06 809154.44

rome@dejalex.com

1170 **BRUXELLES**
Chaussée de La Hulpe 187
tel. +32 (0)2 645 5670
fax +32 (0)2 742 0138

brussels@dejalex.com

115114 **MOSCA**
Ulitsa Letnikovskaya, 10
tel. +7 495 792 54 92
fax +7 495 792 54 93

moscow@dejalex.com

DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

The British Chamber of Commerce for Italy

QUALI SONO I RISCHI/COSTI PER LE AZIENDE IN CASO DI NON COMPLIANCE?

Myriam Desnus, Studio Legale De Berti Jacchia Franchini Forlani

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

RISCHI/COSTI PER LE AZIENDE IN CASO DI NON COMPLIANCE?

QUALI POSSONO ESSERE

SECONDO VOI?

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

SECONDO VOI?

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

...?

RISCHI/COSTI

Sanzioni amministrative, civili e penali

Danni indiretti

- Danno reputazionale
- Costi legali relativi ad azioni giudiziarie
- Possibili impatti su operazioni di M&A
- Costi assicurativi

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

RISARCIMENTO DEL DANNO CODICE PRIVACY E REGOLAMENTO A CONFRONTO

Art. 15 Codice Privacy

- Chiunque cagioni un danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 c.c.

Art. 82 Regolamento

- 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

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

RESPONSABILITA'
PER IL DANNO CAGIONATO – ART. 82

Titolare del trattamento

- Risponde per il danno cagionato dal suo trattamento in violazione del Regolamento

Responsabile del trattamento

- Risponde se non ha adempiuto agli obblighi specificatamente rivolti ai responsabili del trattamento oppure se ha agito in modo difforme o in contrasto rispetto alle legittime istruzioni del titolare

Responsabilità solidale: "per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato"

CONDIZIONI GENERALI PER INFLIGGERE SANZIONI AMMINISTRATIVE PECUNIARIE Art. 83

- Le sanzioni amministrative pecuniarie devono essere **effettive**, **proporzionate** e **dissuasive** (Art. 83, comma 1).
- Viene fornito un lungo elenco di **criteri** da prendere in considerazione per commisurare tali sanzioni (Art. 83, comma 2), quali ad esempio: la natura, gravità e durata della violazione; il carattere doloso o colposo della violazione; le misure adottate per attenuare il danno, le eventuali precedenti violazioni commesse; il grado di cooperazione con l'autorità di controllo; le categorie di dati personali interessate dalla violazione; la maniera in cui l'autorità di controllo ha preso conoscenza della violazione; il rispetto di eventuali precedenti provvedimenti.

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

INASPRIMENTO DELLE SANZIONI PECUNIARIE - ART. 83, COMMA 4

Fino a 10.000.000 EUR o per le imprese fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente

VIOLAZIONI

- degli obblighi del titolare e del responsabile
- degli obblighi dell'organismo di certificazione
- degli obblighi dell'organismo di controllo

INASPRIMENTO DELLE SANZIONI PECUNIARIE - ART. 83, COMMI 5 E 6

Fino a 20.000.000 EUR o per le imprese fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente

VIOLAZIONI

- dei principi di base del trattamento
- dei diritti degli interessati
- dei trasferimenti verso paesi terzi o un'organizzazione internazionale
- di qualsiasi obbligo ai sensi delle legislazioni degli Stati Membri per specifiche situazioni di trattamento
- dell'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi dei dati dell'autorità di controllo o relative al negato accesso [relativamente ai suoi poteri di indagine]
- dell'inosservanza di un ordine da parte dell'autorità di controllo [relativamente ai suoi poteri correttivi, ivi inclusi gli ordini di ingiunzione di una sanzione]

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

INASPRIMENTO DELLE SANZIONI – ESEMPI
Codice Privacy e Regolamento a confronto

	CODICE PRIVACY	REGOLAMENTO
Omessa o inidonea informativa dell'interessato	Da 6.000 a 36.000 EUR*	Fino a 20.000.000 EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente
Omessa comunicazione di una violazione dei dati personali all'interessato	Da 150 a 1.000 EUR per ogni contraente o persone interessata e fino al 5% del volume d'affari realizzato dal fornitore di servizi telefonici e di accesso a Internet nell'ultimo esercizio chiuso anteriormente alla notificazione della violazione*	Fino a 10.000.000 EUR o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente
Inosservanza dei provvedimenti del Garante	Da 30.000 a 180.000 EUR*	Fino a 20.000.000 EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente
	* Art. 164-bis (casi di minore gravità e ipotesi aggravate)	

ALTRE SANZIONI – ART. 84

- Possibilità per gli Stati Membri di adottare altre sanzioni (in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie) da notificare alla Commissione al più tardi entro il 25 maggio 2018.
- Tali sanzioni dovranno essere effettive, proporzionate e dissuasive.
- Tra queste "altre" sanzioni, ovviamente, possono rientrare le **sanzioni penali** in base al *considerando* 149 del Regolamento.
- Le sanzioni penali, ai sensi del predetto *considerando*, dovrebbero poter essere adottate dagli Stati Membri non solo per le violazioni del Regolamento, ma anche per la violazione di norme nazionali adottate in virtù e nei limiti dello stesso, fermo restando il rispetto del principio del *ne bis in idem*.

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

SANZIONI PENALI ATTUALMENTE PREVISTE DAL CODICE PRIVACY

Gli **illeciti penali** relativi ai dati personali sono per ora contemplati dagli artt. 167 e ss del Codice Privacy.

- Le principali fattispecie incriminatrici riguardano il trattamento illecito di dati, le falsità nelle dichiarazioni e notificazioni al Garante, le misure di sicurezza e l'inosservanza di provvedimenti del Garante.

- La condanna per uno dei delitti previsti dal Codice comporta la pena accessoria della pubblicazione della sentenza.

DE BERTI ■ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

AUMENTO CONSIDEREVOLE DEL RISCHIO DI ESSERE SANZIONATI

Principio di *accountability* ➡ rischio elevato di sbagliare

- Valutazione dei rischi rimessa al titolare del trattamento
- L'autorità di controllo potrà dunque sempre ritenere insufficiente la valutazione fatta
- Controllo *ex post* dell'autorità di controllo (salvo in caso di consultazione preventiva ex Art. 36)
- Misure di sicurezza non più minime ma adeguate
- Presunzione di colpa superata solo se il titolare o il responsabile dimostri di non essere imputabile "in alcun modo" (Art. 82.3) dell'evento dannoso
- Possibile ispezione a seguito di notifica all'autorità di controllo in caso di *data breach* (Art. 33)

DANNI INDIRETTI

Danno reputazionale

Gli attacchi informatici e altre forme di perdita di dati possono comportare la perdita non solo di denaro ma anche di credibilità. Il rischio del danno reputazionale aumenta notevolmente a seguito dell'introduzione nel Regolamento per tutti i titolari (e non più solo per i fornitori di servizi telefonici e di accesso a Internet ex Art. 32-bis Codice, nonché in tema di biometria, dossier sanitario elettronico e PA a seguito di Provv. adottati dal Garante) dell'obbligo di **notifica** all'autorità di controllo in caso di ***data breach*** *(*Art. 33 Regolamento), nonché, nei casi più gravi di *data breach*, dell'obbligatoria **notifica** della violazione **anche** agli **interessati**, che espone altresì il titolare o il responsabile alla richiesta di risarcimento del danno (Art. 34 Regolamento).

DANNI INDIRETTI

Costi legali relativi ad azioni giudiziarie

Possibili impatti sulle operazioni di M&A

(Rischio di perdita di dati contenuti nella *data room* virtuale in fase di *due diligence*, impatti della *non compliance*, di precedenti *data breach* e provvedimenti sul prezzo dell'operazione, …)

Aumento dei costi assicurativi

MYRIAM DESNUS

m.desnus@dejalex.com
www.dejalex.com

20121 Milano
Via San Paolo 7
Tel. +39 02 72554.1
Fax +39 02 72554.500

20121 **MILANO**
Via San Paolo, 7
tel. +39 02 72554.1
fax +39 02 72554.500

milan@dejalex.com

00198 **ROMA**
Via Vincenzo Bellini, 24
tel. +39 06 809154.1
fax +39 06 809154.44

rome@dejalex.com

1170 **BRUXELLES**
Chaussée de La Hulpe 187
tel. +32 (0)2 645 5670
fax +32 (0)2 742 0138

brussels@dejalex.com

115114 **MOSCA**
Ulitsa Letnikovskaya, 10
tel. +7 495 792 54 92
fax +7 495 792 54 93

moscow@dejalex.com

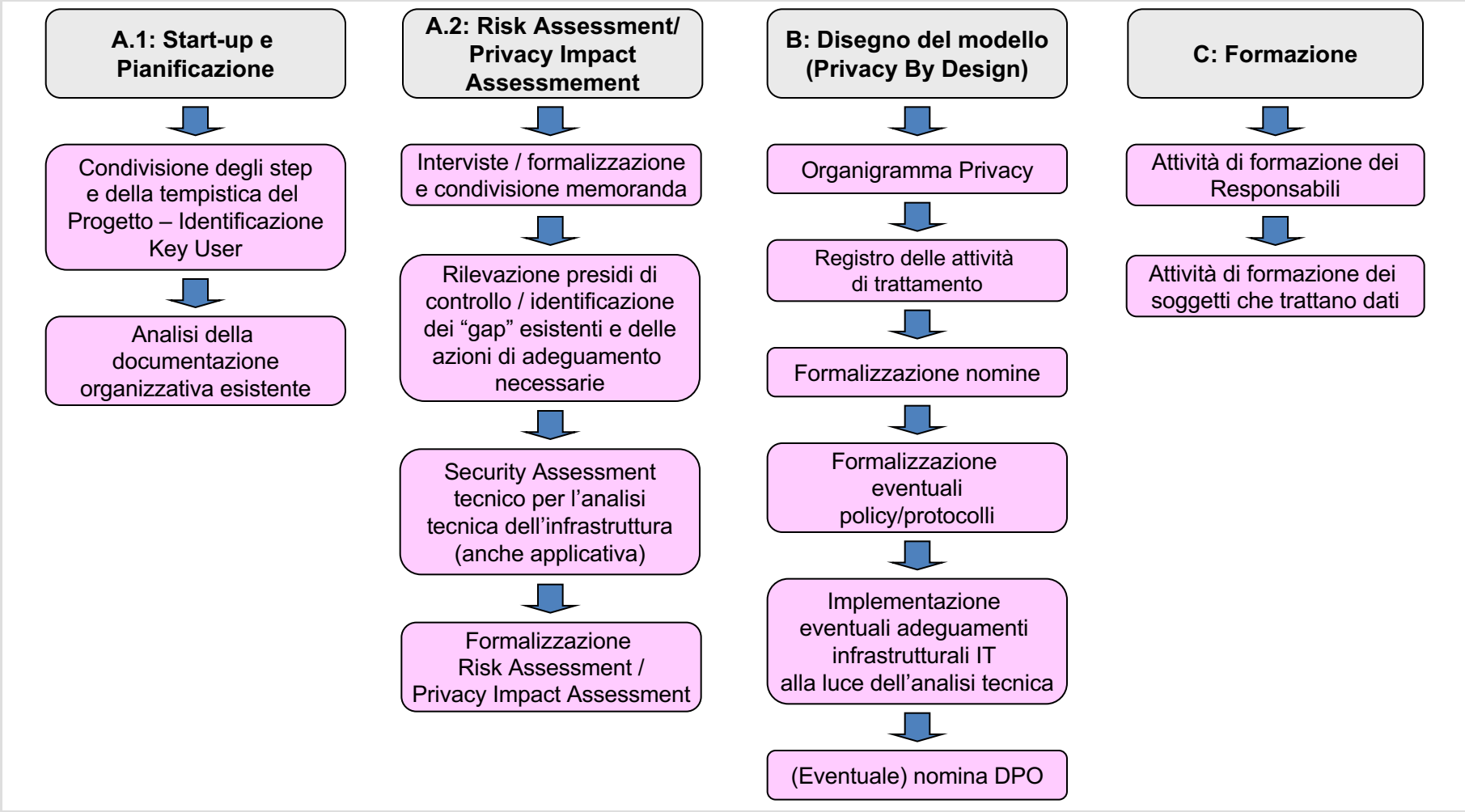
DE BERTI ■ JACCHIA

De Berti Jacchia Franchini Forlani
studio legale

SVILUPPO PROGRAMMA COMPLIANCE

DE BERTI ▪ JACCHIA
De Berti Jacchia Franchini Forlani
studio legale

SVILUPPO DEL PROGRAMMA COMPLIANCE REGOLAMENTO PRIVACY



20121 **MILANO**
Via San Paolo, 7
tel. +39 02 72554.1
fax +39 02 72554.500

milan@dejalex.com

00198 **ROMA**
Via Vincenzo Bellini, 24
tel. +39 06 809154.1
fax +39 06 809154.44

rome@dejalex.com

1170 **BRUXELLES**
Chaussée de La Hulpe 187
tel. +32 (0)2 645 5670
fax +32 (0)2 742 0138

brussels@dejalex.com

115114 **MOSCA**
Ulitsa Letnikovskaya, 10
tel. +7 495 792 54 92
fax +7 495 792 54 93

moscow@dejalex.com