(ALLEGATO N°1)

Informativa GDPR

Acknowledgments – GDPR 679/2017- Rev. 2k18.1

04 Giugno 2018

Sistemia di Leone Stefano Fabio
P.IVA 03404430872
R.E.A. 0232517
Via F.Pensavalle,21 – 95128 Catania (Italy)
Tel. 095.7169500
Fax. 095.7286819
E-Mail: mbox@sistemia.com
Web: www.sistemia.com

Indice

Indice delle Figure

Tabella dei Contenuti

Introduzione – GDPR 679/2017

Che cos'è?

Il Regolamento Generale sulla protezione dei dati (General Data Protection Regulation, GDPR) dell'UE incrementa i requisiti di protezione dei dati personali dei cittadini dell'UE.

Chi riguarda?

Tutte le organizzazioni in possesso di dati che possono portare all'identificazione personale di cittadini dell'UE (ad es. indirizzi e-mail, foto o informazioni cliniche).

Quali sono le tempistiche?

Termine ultimo: Maggio 2018 (anche se in diversi paesi l'implementazione è stata anticipata).

Quali sono i motivi di preoccupazione?

Sanzioni che possono raggiungere i 20 milioni di EUR o il 4% del fatturato annuo globale (a seconda di quale sia più elevato), in caso di violazione dei dati personali.

L'Adeguamento

Il 4 maggio 2016 è stato pubblicato nella Gazzetta ufficiale dell'Unione Europea il "Regolamento (UE) 2016/679 del Parlamento Europeo e del consiglio, del 27 aprile 2016, relativo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il nuovo regolamento abroga la precedente direttiva 95/46/CE (regolamento sulla protezione dei dati) e prende il posto del D. Lgs. 196/03 (Codice della Privacy).

Lo scopo principale del nuovo Regolamento, oltre all'adeguamento della norma all'avvento delle nuove e sempre più pervasive tecnologie, è l'armonizzazione della disciplina sul trattamento dei dati nei diversi paesi europei, così da garantire un'efficace protezione ai cittadini rimuovendo contestualmente gli ostacoli alla circolazione dei dati personali nell'Unione Europea.

Il Regolamento è entrato in vigore il 25 maggio 2016 e, senza necessità di recepimento da parte dei diversi stati membri, sarà pienamente operativo **a partire dal 25 maggio 2018**.

Ciò impone alle aziende una revisione delle politiche sul trattamento dei dati al fine di adeguare la propria organizzazione alle nuove regole **entro il 25 maggio 2018**.

Il 25 maggio 2018, dunque, entrerà in vigore il nuovo Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali e privacy. Imprese e soggetti pubblici dovranno far fronte ad una serie di adempimenti organizzativi per prendere in carico le novità introdotte da questa norma.

Il regolamento introduce il concetto di "responsabilizzazione" (accountability) di titolari e responsabili che devono operare affinché sia dimostrata l'adozione di misure finalizzate ad assicurare l'applicazione del regolamento (artt. 23-25, e Capo IV del regolamento).

In pratica non si tratterà solo di una semplice attività di adeguamento alle norme di legge, quanto una vera e propria "responsabilizzazione" che verrà implementata e consolidata nel corso del tempo.

Viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali nel rispetto delle disposizioni normative.

Tra i criteri ispiratori il principale è "**data protection by default and by design**" che, per ciascun trattamento, debbano essere stabilite fin dall'inizio le garanzie indispensabili per il rispetto dei requisiti del regolamento e la tutela dei diritti degli interessati. Questo criterio richiede, pertanto, un'analisi preventiva che specifichi misure ed obblighi in relazione al rischio, preventivamente identificato, associato al trattamento.

I rischi associati al trattamento sono da intendersi in relazione agli impatti negativi sulle libertà e i diritti degli interessati; questi impatti dovranno essere analizzati attraverso un processo di assessment (DPIA - Data protection impact assessment) che consideri misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di poter adottare per mitigare tali rischi.

L'esito di questa valutazione di impatto sarà indispensabile per avviare il trattamento con l'adozione delle misure di sicurezza necessarie a salvaguardare i dati personali.

Il titolare potrà altresì consultare l'autorità di controllo competente per ottenere indicazioni sulla gestione del rischio residuale. In tal caso l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori da implementare e, se previsto, adottare tutte le misure correttive ai sensi dell'art. 58.

Altri importanti adempimenti da parte di titolari e responsabili del trattamento sono:

- **Registro dei trattamenti**: Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (art. 30, § 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Scopo del registro è disporre di uno strumento utile ai fini dell'eventuale supervisione da parte del Garante e di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico per i controlli e gli adempimenti necessari. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante. Indipendentemente dall'obbligo di tenuta del registro, i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, sarebbero avvantaggiati nella tenuta del registro che garantisce un quadro esaustivo dei trattamenti svolti e dei rischi associati.

- **Misure di sicurezza**: Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva. Sono, dunque, abolite le 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. L' Autorità potrà valutare la definizione di linee-guida o buone prassi mentre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste.

- **Notifica delle violazioni di dati personali**: A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati. Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati.

- **Responsabile della protezione dei dati**: La designazione di un "responsabile della protezione dati" (RPD), ovvero DPO (Data Protection Officer) è finalizzata a facilitare l'attuazione del regolamento da parte del titolare/del responsabile. Fra i principali compiti del RPD rientrano "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto prevista dall'art. 35. La sua designazione è obbligatoria nei casi previsti dall'art. 37, e il regolamento specifiche le competenze e le caratteristiche (indipendenza, autorevolezza, competenze manageriali).

Queste dunque le domande a cui oggi l'azienda è chiamata a dover rispondere:

- Siete a conoscenza dei nuovi obblighi in materia di protezione dei dati personali?
- Disponete di dati personali relativi a cittadini dell'Unione Europea, ad esempio coordinate bancarie, informazioni di contatto o cartelle cliniche?
- Ritenete di rispettare i requisiti relativi alla protezione dei dati personali inclusi nel nuovo Regolamento europeo di imminente attuazione?
- In che misura ritenete di essere conformi al nuovo Regolamento europea sulla protezione dei dati?
- In che modo proteggete i dati personali di cui disponete?
- Siete conformi al nuovo Regolamento europea sulla protezione dei dati? (È applicabile anche ad aziende con sede al di fuori dell'Unione Europea)

Figura 1: I Vantaggi per il cittadino Europeo

Figura Chiave: Il Responsabile della Protezione dei Dati personali (RPD)

Anche conosciuto in inglese Data Protection Officer (DPO), è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. È il soggetto incaricato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto, controllo, consultive, formative e informative relativamente all'applicazione del Regolamento. Coopera con l'Autorità, quindi il suo nominativo va comunicato al Garante e costituisce il punto di contatto (artt. 38 e 39 del Regolamento) anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali.

- Quando non importa designare un RDP (DPO)

  In relazione a "trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria""

- Quando deve essere utilizzata la figura del RDP (DPO)

  nel caso sussista l'attività di "monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.)"

- Figura interna o esterna

  Il soggetto RDP (DPO) "**può essere ricoperto da un dipendente** del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti con atto di designazione; l'incarico può essere **anche affidato a soggetti esterni**, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento, con contratto di servizi. **Tali atti, da redigere in forma scritta**, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento."

  Il Responsabile del Trattamento "dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale".

- Persona o soggetto giuridico

  Se il Responsabile del Trattamento è un dipendente del titolare o del responsabile del trattamento, potrà "essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti."
  Nel caso sia un soggetto esterno, è previsto anche l'utilizzo di una persona giuridica. Si raccomanda, in ogni caso, di procedere a una chiara ripartizione di competenze, individuando una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di controllo.

- Responsabilità nei confronti del trattamento dei dati

  In ogni caso, il Titolare del Trattamento ed il Responsabile del Trattamento, rimangono **responsabili dell'osservanza** della normativa

Nel caso di un gruppo imprenditoriale il Garante ha chiarito che vi è la possibilità di nominare un unico responsabile della protezione dei dati personali a condizione che tale responsabile sia facilmente raggiungibile da ciascuno stabilimento, sia in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

DPIA – Data Protection Impact Assessment

E' uno strumento importante in termini di responsabilizzazione in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGDP, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni.

La responsabilità del DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione (DPO).

Qualora sia necessario il titolare dovrà interfacciarsi con esperti del settore quali il responsabile della sicurezza dei sistemi informativi e il responsabile It.

In breve

Figura 2: GDPR

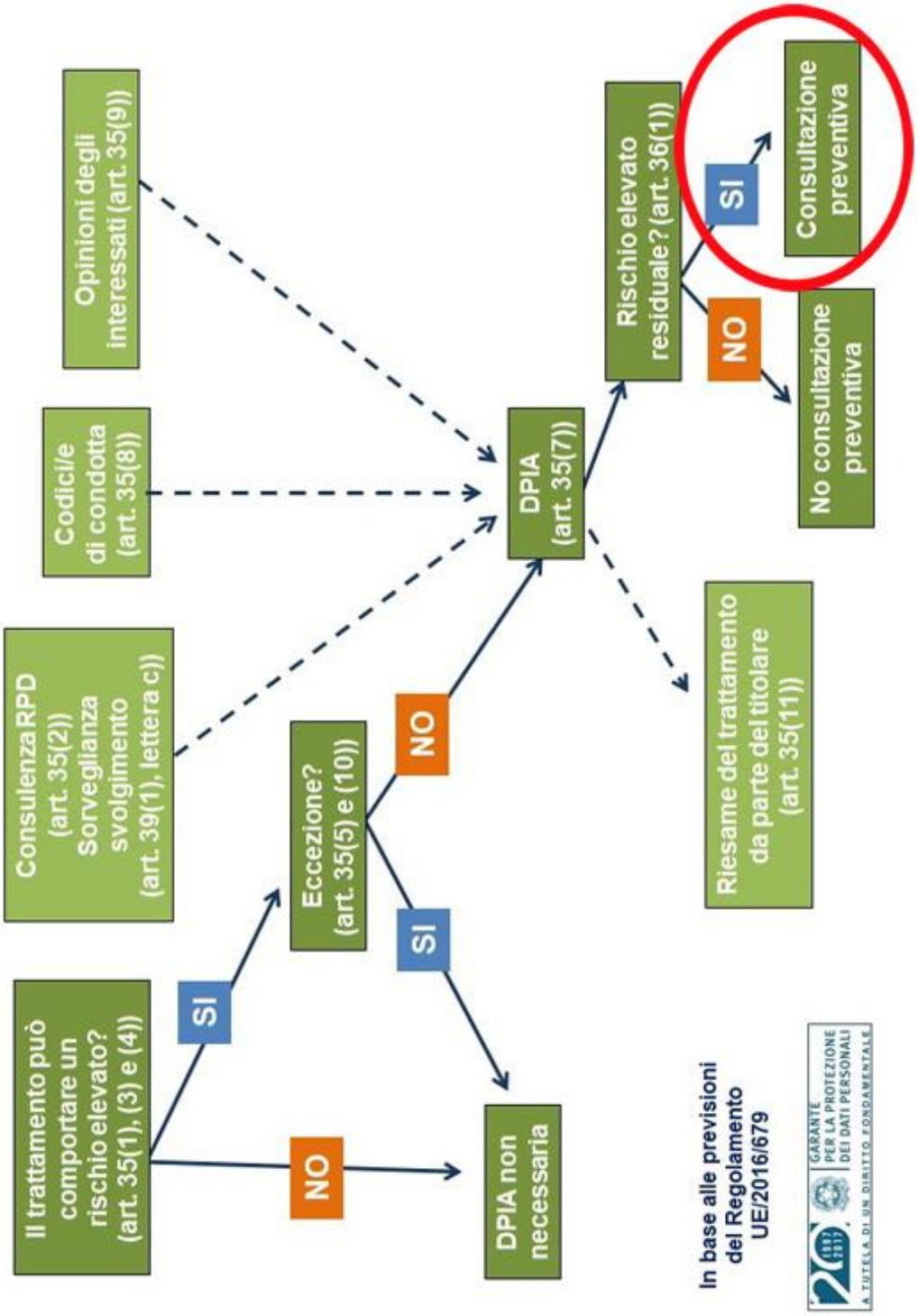

Figura 3: Schematizzazione

Il Regolamento Generale sulla Protezione dei Dati (GDPR) sostituisce la direttiva EU del 1995 sulla protezione dei dati 95/46/EC.

Il GDPR è stato realizzato per potenziare e unire i diritti sulla privacy online e la protezione dei dati personali all' interno dell'Unione Europea (EU) e al tempo stesso velocizzare gli obblighi delle imprese al servizio dei cittadini EU in materia di protezione dei dati attraverso la diffusione di un unico Regolamento al posto delle 28 leggi nazionali.

L'8 Aprile del 2016 il Consiglio ha adottato il GDPR e la Direttiva a questo associata e il successivo 14 Aprile sono stati adottati anche dal Parlamento Europeo.

Il 4 Maggio 2016, i testi ufficiali del Regolamento e della Direttiva sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea. Il Regolamento verrà applicato a partire dal 25 Maggio 2018.

I 28 Stati Membri dell'Unione Europea hanno recepito e attuato le normative del 1995 con notevoli differenze, rendendo difficile e costoso per le imprese operare all'interno dei confini della Comunità Europea. Si stima che l'eliminazione di questa frammentazione porterà a un risparmio per le aziende di circa 2,3 miliardi di euro l'anno in tutta l'Unione Europea.

Quali cambiamenti ci saranno?

I principali cambiamenti previsti dalla riforma includono[1]:

- Il diritto di conoscere quando i dati di un individuo sono stati violati: le aziende e le organizzazioni devono segnalare all'autorità di supervisione nazionale per le violazioni dei dati quali sono gli individui in pericolo e comunicare alla persona interessata tutte le violazioni ad alto rischio nel più breve tempo possibile, di modo che gli utenti possano adottare le adeguate contromisure.
- Migliorare l' applicazione delle regole: le autorità per la protezione dei dati dovranno essere in grado di multare le imprese non conformi alle normative EU fino al 4% del loro fatturato annuo totale. Le sanzioni amministrative non sono obbligatorie e nel caso si decida di imporle dovranno essere decise caso per caso e dovranno essere efficaci, proporzionate e dissuasive.
- Un continente, una legge: un'unica legge pan-europea per la protezione dei dati, che sostituisce il mosaico formato da tutte le leggi nazionali. Le aziende dovranno confrontarsi con un'unica legge, non 28. I benefici sono stimati in 2.3 miliardi di euro l'anno.
- Le organizzazioni devono segnalare all'autorità nazionale le gravi violazioni di dati il prima possibile (meglio se entro 24 ore).
- Il Regolamento si applica integralmente anche alle aziende situate fuori dall'Unione Europea che operano nel mercato comunitario, offrono servizi e prodotti ai cittadini europei (inclusi i beni e i servizi gratuiti), e infine controllano il comportamento degli individui dell'Unione Europea.
- Protezione dei dati in fase di progettazione e in modalità predefinita: 'la protezione dei dati by design' e 'la protezione dei dati by default' ora sono elementi essenziali nelle regole di protezione dei dati dell'Unione Europea. La garanzia sulla protezione dei dati sarà prevista nei prodotti

1 Comunicato Stampa: http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

e nei servizi già dalle prime fasi del loro sviluppo e le impostazioni predefinite per la tutela della privacy saranno la norma.

Per rafforzare la protezione dei dati, l'Unione Europea sta rendendo obbligatorio per le aziende proteggere adeguatamente i dati riservati definiti come:

> *"qualsiasi informazione che identifichi o che permetta di identificare una persona fisica a cui ci si riferirà in seguito come "soggetto dei dati"; una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante un numero identificativo o da uno o più fattori specifici relativi alla sua identità fisica, psicologica, mentale, economica, culturale o sociale;"*[2]

Questa ampia definizione dei dati personali si estende facilmente ai documenti più semplici che riguardano persino indirettamente i clienti, gli utenti, il personale, gli studenti e ogni altro documento relativo all'individuo.

Cosa dice il Regolamento sulla Protezione dei Dati?

Articolo 32, Sicurezza nel trattamento dei dati [3]:

> 1. Considerando lo stato dell'arte, i costi di implementazione, la loro natura, la loro portata, il contesto e le finalità del trattamento dei dati, come anche le variabili legate ai rischi per i diritti e la libertà delle persone fisiche, il sistema di controllo e trattamento dei dati verrà implementato con misure tecniche e organizzative per assicurare un livello di sicurezza adeguato ai rischi, che include a seconda dei casi:
>
> *a) l'utilizzo di pseudonimi e la crittografia dei dati personali;*
> *b) la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione;*
> *c) la capacità di ripristinare la disponibilità e l'accesso ai dati personali in maniera tempestiva in caso di incidenti fisici o tecnici;*
> *d) un processo di controllo periodico e la valutazione dell'efficienza dei mezzi tecnici per verificare la sicurezza dell'elaborazione.*

La crittografia è il modo più semplice e sicuro per proteggere i dati come richiesto dall'Articolo 32 del GDPR. La tecnologia è uno dei mezzi stabiliti per proteggere le informazioni che possono essere oggetto di furti o smarrimenti. Il GDPR tratta anche l'esigenza di avere degli efficaci piani per il ripristino dei dati, delle password e dei sistemi di gestione delle chiavi.

L'articolo 30 del Regolamento[3] richiede inoltre che i documenti siano conservati, inclusa una descrizione generale delle misure di sicurezza tecniche e organizzative adottate di cui all'Articolo 32, questo significa che le imprese avranno bisogno della documentazione e delle prove che i loro sistemi sono sicuri e che i dati criptati sono recuperabili dopo un incidente tecnico.

2 REGOLAMENTO (EC) No 45/2001: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2001.008.01.0001.01.ENG

3 Testo del Reolamento: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Quali sono le regole per la segnalazione della violazione dei dati?

L'Articolo 33[3] prevede la notifica di una violazione dei dati personali all'autorità di vigilanza e stabilisce che l'autorità venga avvisata, ove fattibile, entro e non oltre 72 ore dal momento in cui l'organizzazione in questione viene a conoscenza della violazione stessa. Qualsiasi notifica oltre le 72 ore deve essere accompagnata da una motivazione che ne giustifichi il ritardo.

L'Articolo 34[3] si riferisce alla comunicazione della violazione dei dati personali al soggetto interessato e afferma che:

> 1. *Nel caso in cui la violazione dei dati personali possa comportare un rischio elevato per i diritti e le libertà delle persone, il controllore dovrà comunicare tale violazione al proprietario dei dati senza indebito ritardo.*

Tuttavia prosegue affermando che:

> 3. *La comunicazione al proprietario dei dati, come indicato nel paragrafo 1, non sarà richiesta se viene rispettata almeno una delle seguenti condizioni:*
>
> *a) il titolare del trattamento ha implementato appropriate misure di protezione tecniche e organizzative e queste misure sono state applicate ai dati personali oggetto della violazione. Si fa particolare riferimento a quelle tecnologie che rendono i dati personali illeggibili per qualsiasi persona non autorizzata ad accedervi, come ad esempio la crittografia;*
>
> *b) il controllore ha adottato successive misure tali da assicurare che l'elevato rischio per i diritti e le libertà delle persone, come indicato nel paragrafo 1, non si possa concretizzare;*
>
> *c) comporta uno sforzo sproporzionato. In questo caso ci sarà una comunicazione pubblica o di natura simile in grado di informare le persone interessate in maniera altrettanto efficace.*

Alcune ricerche hanno dimostrato che, nelle precedenti violazioni dei dati, le conseguenze più gravi sono ai danni dell'organizzazione coinvolta. Anche in questo caso, è chiaro che la crittografia viene considerata una garanzia sufficiente a evitare questa situazione e le conseguenze per la reputazione dell'azienda.

In che modo il Regolamento scoraggia i trasgressori?

Articolo 83, Condizioni generali per l'imposizione di sanzioni amministrative- punto 4[4]:

> 4. *Le infrazioni alle seguenti disposizioni, ai sensi del paragrafo 2, sono soggette a sanzioni amministrative fino a 10 000 000 di euro, o in caso si tratti di un'azienda, fino al 2% del suo fatturato totale a livello mondiale riferito all'anno precedente, a seconda di quale sia l'importo più alto:*
>
> *a) gli obblighi del titolare e del responsabile del trattamento ai sensi degli Articoli 8, 11, dal 25 al 39, 42 e 43;*

il punto 5 dell'Articolo 83 inoltre afferma che:

> 5. *Le infrazioni alle seguenti disposizioni, in accordo con il paragrafo 2, saranno oggetto di sanzioni amministrative fino a 20 000 000 euro, o nel caso si tratti di un'azienda, fino al 4 % del suo fatturato totale a livello mondiale riferito all'anno precedente, a seconda di quale sia l'importo più alto:*
>
> *a) i principi base del trattamento dei dati, incluse le condizioni per il consenso, ai sensi degli Articoli 5, 6, 7 e 9;*

Dove all'Articolo 5, Principi relativi al trattamento dei dati personali,si afferma che:

> 1. *I dati personali dovranno essere:*
>
> *f) trattati in modo da garantirne un'adeguata sicurezza - inclusa la protezione dal trattamento non autorizzato o illegale nonché dalla perdita accidentale, distruzione o danno - utilizzando appropriate misure tecniche o organizzative (integrità e riservatezza).*

Questo chiaro intento di penalizzare e scoraggiare i trasgressori entrerà in vigore a Maggio 2018, quindi è arrivato il momento di agire.

Alcuni paesi sono già al lavoro. Il Senato Olandese ha approvato una legge a Maggio 2015 che modifica l'attuale legge sulla protezione dei dati per anticipare l'adozione del GDPR, facendo passare l'Olanda da paese con un sistema di attuazione tra i più deboli d'Europa a uno di quelli che tra i più forti. Il Regolamento entrerà in vigore in tutti i 28 stati membri da Maggio 2018.

4 Testo del Regolamento: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

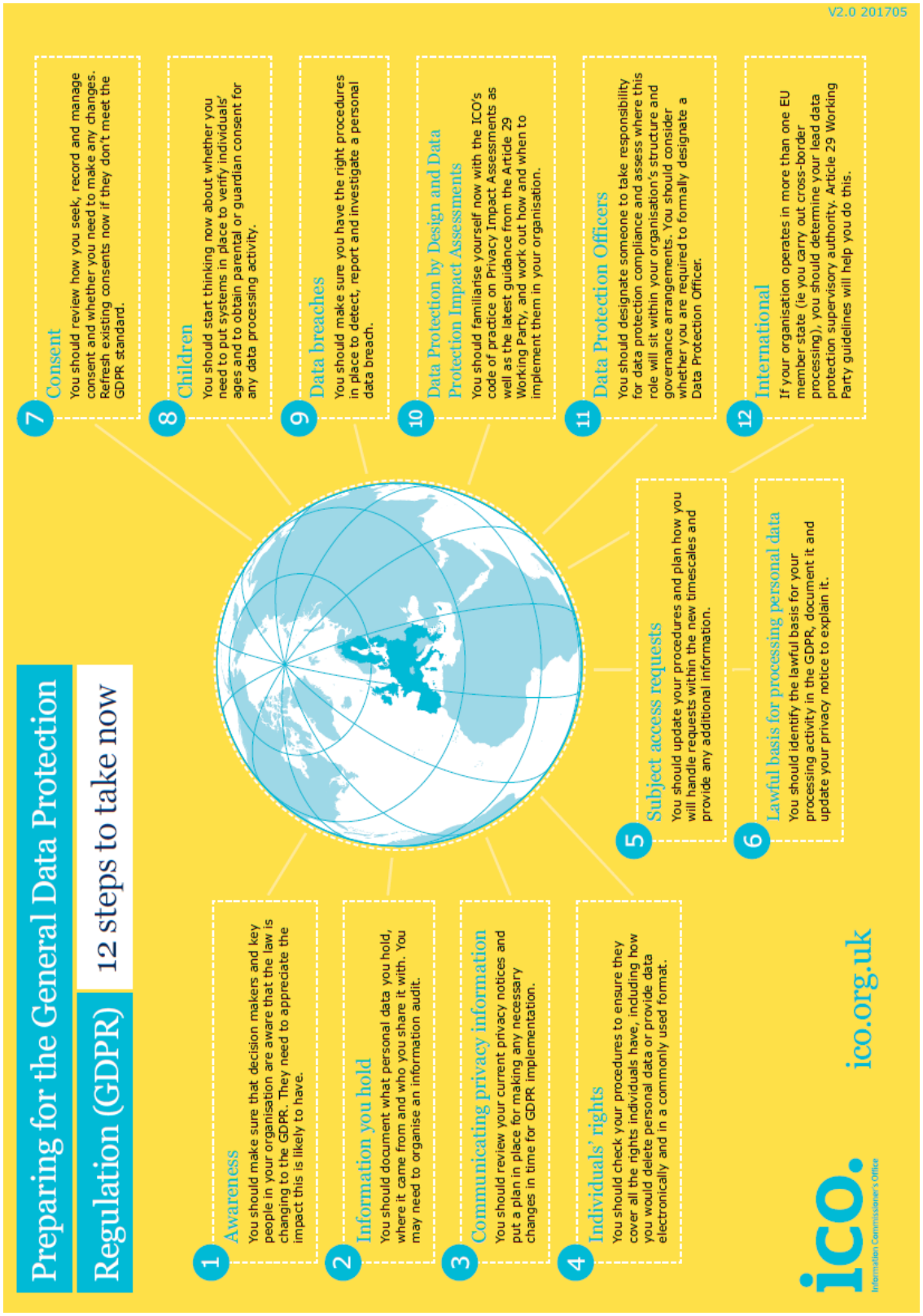

Figura 4: 12 Steps di preparazione

LE AZIENDE DEVONO

- Proteggere i dati personali dei clienti da accessi non autorizzati (breach);
- Istruire tutto il personale dipendente in merito alla nuova normativa;
- Adottare una politica di governance e data protection adeguata in modo proporzionale al rischio in caso di breach;
- Introdurre la figura del DPO, il Data Protection Officer, che può essere interno o esterno all'azienda a seconda dei casi;
- Dotarsi di strumenti tecnologici necessari a monitorare e prevenire gli attacchi informatici.

I PROPRIETARI DEVONO POTER

- Accedere in qualsiasi momento ai loro dati personali;
- Essere informati in merito all'utilizzo e protezione dei loro dati;
- Chiedere il trasferimento dei loro dati personali ad un altro soggetto (portabilità del dato);
- Essere informati tempestivamente in caso di furto dei propri dati;
- Avere garanzie sull'applicazione della normativa da parte dei soggetti interessati.

Le Sanzioni previste

In materia di protezione dei dati personali, il regolamento Gdpr richiede all'azienda di adottare un sistema di policy, misure organizzative e tecniche che consentano di avere un controllo continuo sulla conformità dell'azienda stessa alla normativa. Qualora ciò non accadesse o anche nel caso si evidenziasse la mancanza della conformità a quanto disposto dal Regolamento, sono previste precise **sanzioni** amministrative pecuniarie.

Va tuttavia sottolineato che l'adesione ai codici di condotta e la certificazione del trattamento sono elementi di cui l'Autorità deve tener conto nell'applicazione di eventuali sanzioni o nell'analisi della correttezza di una valutazione di impatto effettuata dal titolare del trattamento dei dati.

Sanzioni graduali

Va da sé che le sanzioni seguono un approccio graduale riguardo i criteri per l'imposizione (secondo quanto riportato nell'art. 83, paragrafo 2 del GDPR) e per la determinazione dell'ammontare massimo imponibile.

In termini generali, la violazione delle disposizioni può prevedere **sanzioni amministrative** pecuniarie fino a 20 milioni di euro, oppure per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore alla predetta cifra.

Allo stesso modo l'inosservanza di un ordine da parte dell'autorità di controllo secondo quanto riportato **all'articolo 58**, paragrafo 2 prevede sanzioni amministrative pecuniarie fino a 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Va tuttavia sottolineato che, in linea con quanto previsto dalla legislazione vigente, l'articolo 58 fornisce alle autorità di controllo l'opportunità di avvalersi di una serie di poteri correttivi. In particolare, tra le altre cose è prevista anche la possibilità di **limitare** o addirittura **vietare** un trattamento dei dati.

Oltre le sanzioni amministrative

È facilmente intuibile come una disposizione di questo tipo potrebbe portare a conseguenze economiche ben più gravi di quelle derivanti dalla "semplice" sanzione amministrativa. Infatti, inibire totalmente la possibilità di effettuare il trattamento dei dati potrebbe voler dire dover interrompere l'erogazione di un servizio o un'attività già in atto con ovvie ripercussioni sui clienti, i quali potrebbero quindi adire alle vie legali per ottenere il risarcimento dei danni subiti.

La non conformità alle normative imposte dal Gdpr o un'inadeguata gestione del trattamento dei dati possono quindi comportare una sanzione amministrativa pecuniaria, che può avere un'incidenza anche molto rilevante sia in termini economici sia di immagine. Tuttavia, un intervento delle autorità di controllo, in virtù dei poteri che gli sono stati conferiti, può avere effetti ancor più importanti, rischiando di arrivare nelle situazioni più estreme a compromettere il prosieguo delle attività di un'azienda.