GDPR, lo stretto indispensabile per le associazioni:

Cosa dobbiamo fare per adeguarci al Regolamento europeo per la privacy

Se l’interessato non capisce perché gli chiedete un consenso, il suo consenso non è valido.

Un consenso non può mai essere presunto. Non dissentire non è un consenso. Il silenzio non è un consenso. L'adesione a un'ideale o l'appoggio dato in precedenza a una organizzazione non è un consenso. Il consenso è un consenso.

Regolamento UE 2016/679

- G.D.P.R. = GENERAL DATA PROTECTION REGULATION
- Regolamento per la protezione dei dati personali obbligatorio in tutti i Paesi membri dell'Unione Europea a partire dal 25.5.2018
- Con la sua entrata in vigore cessano tutte le normative nazionali sulla privacy, in Italia D. Lgs. 196/2003

Decreto legislativo n. 101 del 10.8.2018

«Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle perone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

WWW.GARANTEPRIVACY.IT

NOVITA' INTRODOTTE DAL D. LGS. 101/2018

- Sino al maggio 2019 nell'erogare le sanzioni il Garante terrà conto di essere ancora in una fase iniziale di attuazione della normativa
- Il consenso dei minori italiani che abbiano compiuto i 14 anni
- La possibilità per il titolare ed il responsabile di nominare persone fisiche espressamente designate per svolgere specifici compiti e funzioni in relazione al trattamento dei dati personali
- Il consenso nei *curricula* non è dovuto ed l'informativa può essere fornita al momento del primo contatto utile
- Limitazione dei diritti degli interessati
- Gestione dei diritti riguardanti le persone decedute che possono essere esercitati da chi ha un interesse proprio o per ragioni familiari

PRINCIPALI NOVITA’

- PRINCIPIO DI ACCOUNTABILITY ovvero responsabilizzazione/rendicontazione
- PRIVACY BY DESIGN e PRIVACY BY DEFAULT
- D.P.O. = Data Protection Officer
- REGISTRO DEI TRATTAMENTI
- VALUTAZIONE DI IMPATTO
- PROCEDURA DI DATA BREACH
- RILASCIO DEL CONSENSO E POSSIBILITA’ PER I MINORI DI PRESTARE VALIDAMENTE IL LORO CONSENSO
- CONTENUTO DELL’INFORMATIVA
- DIRITTI DELL’INTERESSATO

Principio di ACCOUNTABILITY

«SEI TU, TITOLARE O RESPONSABILE DEL TRATTAMENTO A DOVER DECIDERE SE E QUALI TUE ATTIVITA' SONO SOTTOPOSTE AL GDPR E COSA FARE PER RENDERLE COERENTI CON LO SPIRITO DELLA NORMATIVA»

ATTRAVERSO UNA SELF REGULATION IL TITOLARE DEVE INDIVIDUARE E PORRE IN ESSERE LE MIGLIORI SCELTE PER RAGGIUNGERE L'OBIETTIVO INDICATO DALLA NORMATIVA

DOCUMENTARE TUTTE LE SCELTE EFFETTUATE PER PORRE IN ESSERE L'ADEGUAMENTO RICHIESTO DAL REGOLAMENTO

APPLICARE DETTO PRINCIPIO PER OGNI TRATTAMENTO DEL DATO

METTERE IN ATTO LE POLITICHE E PROCEDURE APPROPRIATE PER DIMOSTRARE LA CONFORMITA'

DATA PROTECTION BY DEFAULT AND BY DESIGN

By design:

- ❑ Pseudonimizzazione
- ❑ Minimizzazione del trattamento
- ❑ Protezione sin dalla progettazione del trattamento

DATA PROTECTION BY DEFAULT AND BY DESIGN

By default:

Il titolare deve trattare solo ed esclusivamente i dati personali nella misura necessaria e sufficiente per le finalità previste e per il trattamento strettamente necessario, garantendo la NON ECCESSIVITA' DEI DATI RACCOLTI

TITOLARE DEL TRATTAMENTO
art. 26 GDPR

E’ la persona fisica o giuridica che determina le finalità e i mezzi del trattamento dei dati personali
E’ tenuto ad adottare e dimostrare di aver adottato tutte le misure necessarie a garantire la conformità del trattamento al GDPR

RESPONSABILE DEL TRATTAMENTO
art. 28 GDPR

E’ la persona fisica o giuridica che tratta dati personali per conto del Titolare del trattamento
E’ una figura esterna all’organizzazione del titolare

La nomina deve avvenire con apposito CONTRATTO O ALTRO ATTO GIURIDICO

DATA PROTECTION OFFICER
art. 37 GDPR

E’ una nuova figura di tipo manageriale che affianca il titolare del trattamento e si occupa in via esclusiva della materia della protezione dei dati personali.

Deve avere una formazione specifica e deve essere designato sulla base di qualità professionali, in particolare della sua conoscenza della legge sulla protezione dei dati e la capacità di compiere le funzioni richieste.

DATA PROTECTION OFFICER
art. 37 GDPR

La nomina del DPO è obbligatoria:

a) Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) Le attività principali del titolare o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
c) Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

DATA PROTECTION OFFICER
art. 37 GDPR

Il DPO si incarica della formazione dei collaboratori, del dialogo con i fornitori e delle eventuali segnalazioni alla Autorità Garante della protezione della privacy.

Il DPO stende le Valutazioni di impatto sulla protezione dei dati (DPIA), le privacy policy e la modulistica.

Il DPO collabora alla definizione dei contratti con clienti e fornitori.

REGISTRO DEI TRATTAMENTI
ART. 30 GDPR

DEVE CONTENERE:

A) Nome e dati di contatto del titolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

B) Finalità del trattamento;

C) Descrizione delle categorie di interessati e delle categorie di dati personali;

D) Categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;

E) Ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie assunte;

F) I termini previsti per la cancellazione delle diverse categorie di dati;

G) Descrizione generale delle misure di sicurezza tecniche ed organizzative.

ESEMPIO
registro semplificato

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SCHEDA REGISTRO DEI TRATTAMENTI *[per i contenuti vedi Faq sul registro delle attività d*

TITOLARE /CONTITOLARE /RAPPRESENTANTE DEL TITOLARE *[inserire la denominazione e i dati di contatto]*

RE SPONSABILE DELLA PROTEZIONE DEI DATI *[inserire la denominazione e i dati di contatto]*

TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERESSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*

Valutazione di impatto
Data Protection Impact Assessment DPIA

- L’art 35 del GDPR introduce l’istituto della valutazione di impatto per i trattamenti che presentano rischi specifici
- E’ uno strumento importante per la responsabilizzazione, poiché è un processo inteso a garantire e dimostrare la conformità al GDPR delle misure adottate per la protezione dei dati personali
- È obbligatoria ogniqualvolta il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche

Dobbiamo davvero fare una DPIA? Per rispondere a questa domanda segnate a fianco se la frase descrive uno o più trattamenti svolti nella vostra associazione.

❑ I dati raccolti sono utilizzati dal Titolare o da terzi per prendere decisioni che producono effetti giuridici (assunzioni, prestiti, assicurazioni, fidi).

❑ I dati raccolti sono utilizzati dal Titolare o da terzi per decisioni che possono impedire agli interessati di avvalersi di un servizio (per esempio scoring per fidi).

❑ I dati raccolti sono utilizzati dal Titolare o da terzi per attività di scoring, valutazione o per profilare gli interessati.

❑ I dati raccolti sono utilizzati dal Titolare o da terzi per attività di profilazione combinazione e raffronto di insiemi di dati provenienti da diverse fonti.

❑ I dati raccolti sono sottoposti a un monitoraggio sistematico (videosorveglianza).

❑ L'organizzazione tratta dati sensibili estremamente personali (giudiziari opinioni politiche).

❑ L'organizzazione tratta dati personali su larga scala (anche videosorveglianza di aree accessibili al pubblico).

❑ L'organizzazione tratta dati relativi a soggetti vulnerabili (minori, dipendenti patologie psichiatriche anziani).

❑ L'organizzazione utilizza soluzioni tecnologiche avanzate (per es.: internet of things, riconoscimento facciale).

❑ L'organizzazione controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.

Se abbiamo segnato almeno due domande dovremmo fare una DPIA.

Le linee guida prevedono che non sia obbligatoria se i trattamenti non presentano rischio elevato per diritti e libertà dell'interessato, se i trattamenti sono simili ad altri per i quali lo stesso soggetto ha già effettuato una DPIA, se sono stati sottoposti a verifica da parte del Garante…

Nell'incertezza è meglio farla!

SANZIONE

La mancata esecuzione, l'esecuzione in maniera errata o la mancata consultazione dell'Autorità di Controllo ove richiesta comporta una sanzione amministrativa pecuniaria fino ad un massimo di 10 milioni di € ovvero se si tratta di una impresa fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

DATA BREACH
ART. 33 GDPR

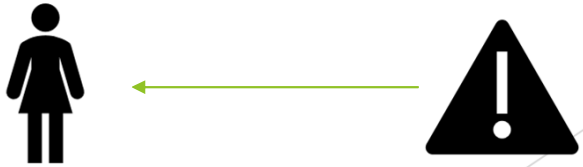
Furto di dati

72 ore

notifica

AUTORITA' DI PROTEZIONE DEI DATI

- Numero registri esposti
- Misure per attenuare effetti negativi
- Categorie dati violati
- Misure per rimedio violazione
- Conseguenze violazione e rischio elevato per diritti e libertà persone



CONSENSO

Il consenso è qualsiasi manifestazione di volontà con la quale l'interessato medesimo presti in maniera libera, specifica, informata ed inequivocabile il proprio assenso «che i dati personali che lo riguardano siano oggetto di trattamento» ricorrendo ad una dichiarazione o, in alternativa, ad una «azione positiva inequivocabile»

Atto positivo ed inequivocabile

- DICHIARAZIONE SCRITTA (ma non necessariamente sottoscritta) approntata anche con mezzi elettronici;
- DICHIARAZIONE ORALE;
- AZIONE POSITIVA NON DICHIARATIVA MA PUR SEMPRE INEQUIVOCABILE in ordine all'accettazione dell'interessato.

Il consenso non deve essere necessariamente documentato per iscritto ma vi è la necessità di documentare l'attività di trattamento svolta.

Il titolare deve dimostrare che l'interessato ha prestato il consenso ad uno specifico trattamento.

INFORMATIVA

CONTENUTI DELL'INFORMATIVA

- 1. Gli estremi identificativi del Titolare del Trattamento e del Responsabile del Trattamento nonché, se esiste del DPO al quale Titolare o Responsabile fanno riferimento.
- 2. La finalità del trattamento e, se non implicita, la relativa base giuridica.
- 3. Se i dati richiesti possono essere soggetti a più trattamenti le finalità e le modalità di ciascuno. In particolare deve essere chiaro in che misura la comunicazione dei dati rappresenti un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto.
- 4. Le modalità del trattamento, con particolare riferimento agli eventuali destinatari o alle eventuali categorie di destinatari dei dati raccolti.
- 5. Se i dati personali potrebbero essere trasferiti, anche in una fase successiva di trattamento, in un Paese esterno all'Unione Europea se questo è giudicato adeguato dalla Commissione europea e la natura di questo trasferimento.
- 6. Il periodo di conservazione dei dati o i criteri per definire tale periodo.
- 7. Se il trattamento dei dati alimenta presso il Titolare o presso terzi un processo decisionale automatizzato, compresa la profilazione per esempio per accedere a determinati prezzi o tipologie di offerta e in tali casi, informazioni significative sulla logica utilizzata e sulle sue potenziali.
- 8. Le conseguenze che il trattamento potrebbe avere sull'interessato.

DIRITTI DELL'INTERESSATO

Nell'informativa deve essere esplicitato che l'interessato dispone di questi diritti:

- Diritto di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi;
- Diritto di limitare il trattamento dei dati che lo riguardano o di opporsi al loro trattamento;
- Diritto di revocare il consenso in qualsiasi momento;
- Diritto di presentare un reclamo alla Autorità di controllo e i dati necessari per farlo.

Check list breve

1. Le persone interessate al cambiamento sanno cosa devono fare? Elencate le persone che nell'organizzazione saranno interessate dalla nuova norma sulla privacy e per quali aspetti. Assicuratevi che sappiano per tempo cosa cambierà nel loro modo di lavorare.

2. So quali dati possediamo e da dove vengono?
Identificate le tipologie di dati delle quali disponete e associateli a delle fonti. Questa attività può richiedere tempo e la consultazione di persone che in passato avevano lavorato con l'organizzazione.

3. Di quali basi legali dispongo per possedere/trattare questi dati? Per trattare dati personali l'organizzazione deve definire quale 'base legale' ritiene di avere. Questo requisito è ancora più stringente se si tratta di dati particolarmente sensibili. Occorre consultare le circostanze proposte dalla normativa e redigere un documento nel quale i responsabili dell'organizzazione dichiarano su quali basi ritengono di poter operare.

Check list breve

4. Chi sono i responsabili? Una persona o un dipartimento all'interno dell'organizzazione deve prendersi la responsabilità del trattamento dei dati. L'organizzazione deve anche valutare se è consigliabile o obbligatorio dotarsi di un consulente esterno specialista (Data protection officer).

5. Ho aggiornato le informative e le richieste di consenso? Elencate tutti i momenti di contatto con l'esterno. Quali hanno bisogno di una informativa e di un consenso? Preparate i testi dell'informativa e delle richieste di consenso.

6. Gli accordi stretti con i fornitori mi coprono da potenziali rischi? Quasi sicuramente dovrete riscrivere i contratti con realtà esterne che lavorano i vostri dati (webmaster, agenzie di direct marketing, agenzie di inoltro postale).

Check list breve

7. Devo chiedere un nuovo consenso a chi mi ha rilasciato dei dati?

Quasi sicuramente sì. Andranno contattate tutte le persone che vi hanno rilasciato direttamente dei dati chiedendo perlomeno un silenzio/consenso. Se i dati provengono da terzi, dovrete chiedere una dichiarazione formale che questi dati sono stati raccolti in ottemperanza al GDPR. Se questo non è possibile dovete contattare direttamente gli interessati.

Check list breve

8. Come posso garantire i miei dati da furti e attacchi informatici?

Il GDPR richiede un riesame attento del modo in cui i dati sono trasmessi e immagazzinati. L'organizzazione deve poter dimostrare di aver fatto tutto quanto ragionevolmente possibile al fine di minimizzare i rischi di alterazione cancellazione copia e diffusione dei dati personali.

Le soluzioni sono diverse: cifratura dei dati durante la trasmissione, suddivisione delle informazioni personali in due database separati con l'utilizzo di codici (pseudonomizzazione) oltre alle misure anti-intrusione e di backup in caso di cancellazione/ manomissione dei dati. Probabilmente non ne sapete nulla ma *ignorantia non excusat*.

Check list breve

9. Cosa succede se un interessato chiede l'accesso o la modifica dei dati?

Insieme ai fornitori che elaborano i vostri dati, definite delle procedure e dei tempi minimi sia in caso di una normale richiesta di accesso/modifica dei dati sia in caso di '*data breach*' cioè di accesso non autorizzato o modifica o cancellazione dei dati stessi.

TEST
DI
AUTOVALUTAZIONE

Il GDPR in generale 1. Le sigle GDPR, RGPD, 2016/679.

- ❑ A. GDPR e RGPD indicano il Regolamento europeo mentre 2016/679 è la legge
- ❑ B. GDPR e RGPD indicano il Regolamento; mentre 2016/679 è la legge italiana che l'ha recepita
- ❑ C. Si riferiscono a tre norme differenti, anche se tutte relative alla privacy
- ❑ D. Sono tre modi di indicare la stessa norma

A. Non è esatto. Si tratta in realtà di tre modi di indicare la stessa norma: 2016/679 è il numero assegnato dal Parlamento europeo alla norma GDPR. B. Non è esatto. Si tratta in realtà di tre modi di indicare la stessa norma: 2016/679 è il numero assegnato dal Parlamento europeo alla norma GDPR.
C. Risposta errata. Si tratta di tre modi di indicare la stessa norma.
D. Risposta esatta: RGPD è la sigla tradotta in italiano mentre 2016/679 è il numero assegnato dal Parlamento europeo.

2. Il GDPR è in pieno vigore...

❑ A. Dal maggio 2016 in altri paesi UE. In Italia si attende ancora la legge che recepisce la normativa

❑ B. In ogni Paese della UE a partire da due anni dopo il 25 maggio 2018

❑ C. In ogni Paese della UE dal 2016 e pienamente efficace dal 25 maggio 2018

❑ D. Solo nei Paesi UE che lo hanno accettato

Il GDPR è in pieno vigore.

A. Non è esatto. Trattandosi di un Regolamento e non di una Direttiva, non ha bisogno di essere recepito
B. Non è esatto. I due anni di tempo concessi per adeguare le norme nazionali e le prassi sono iniziati nel maggio 2016 e terminano nel maggio 2018.
C. Risposta esatta.
D. Non è esatto: il Regolamento è valido in tutti i paesi UE.

3. Il GDPR prende in considerazione…

❑ A. Solo i dati relativi a persone fisiche, in qualunque modo siano raccolti o trattati

❑ B. Tutti i dati specifici relativi a persone fisiche e giuridiche

❑ C. Tutti i dati detenuti da aziende sopra i 250 dipendenti

❑ D. Tutti i dati relativi a persone fisiche raccolti o distribuiti via internet

A. Risposta esatta.
B. Non è esatto. Il GDPR non prende in considerazione i dati relativi a persone giuridiche (aziende, associazioni, enti).
C. Non è esatto. Il GDPR riguarda tutte le organizzazioni, grandi medie, piccole o piccolissime private o pubbliche che siano.
D. Non è esatto. Internet è la principale fonte di rischi per la privacy ma il GDPR prende in considerazione ogni modalità di raccolta e trattamento dei dati personali.

4. Le sanzioni previste dal GDPR…

❑ A. Non sono ancora state definite e quindi non possono essere comminate

❑ B. Sono state definite e sono poco più che simboliche

❑ C. Sono state definite, sono potenzialmente molto alte e scattano anche senza un danno alla privacy

❑ D. Sono state definite, sono rilevanti ma scattano solo di fronte a una denuncia o se succede un guaio

A. Non è esatto. Ogni Autorità nazionale deve definire delle Linee Guida per precisarne l'irrogazione (e l'Italia non le ha ancora emanate), ma le sanzioni esistono già e possono essere comminate dalla mattina del 26 maggio 2018.
B. Risposta errata. La norma definisce sanzioni massime molto pesanti: 20 milioni di euro o il 4% del giro d'affari dell'organizzazione.
C. Risposta esatta: le sanzioni possono arrivare a 20 milioni di euro o al 4% del giro d'affari dell'organizzazione.
D. Non è esatto. Nulla nella norma fa pensare che le sanzioni possano scattare solo in caso di denuncia da parte di un interessato o solo in caso di incidente (furto di dati).

5. Il GDPR quando parla di ‘trattamento dei dati’, si riferisce…

❑ A. A ogni dato personale raccolto, indipendentemente dal fatto che venga utilizzato o meno

❑ B. Solo agli utilizzi fraudolenti dei dati personali

❑ C. Solo ai dati personali che vengono effettivamente utilizzati

❑ D. Solo ai dati personali raccolti senza alcuna forma di consenso

A. Risposta esatta.
B. Risposta errata. Il GDPR copre ogni dato raccolto, indipendentemente dal fatto che venga utilizzato o meno e indipendentemente dalla legittimità dell’utilizzo che se ne fa.
C. Non è esatto. Il termine ‘trattamento’ comprende anche la raccolta o detenzione di un dato, indipendentemente dal fatto che venga utilizzato o meno.
D. Risposta errata. IL GDPR copre ogni dato raccolto, indipendentemente dalla presenza di un consenso e perfino dal fatto che venga utilizzato o meno.

6. Titolare del trattamento...

❑ A. È l'autorità Garante della privacy

❑ B. È l'organizzazione che fisicamente possiede i dati

❑ C. È l'organizzazione che ha il potere di decidere quali dati raccogliere e cosa farne

❑ D. È un esperto esterno che l'organizzazione incarica e che si assume la responsabilità

A. Risposta errata. Il Titolare è l'organizzazione che deve adempiere al GDPR.
B. Non è esatto. Possedere i dati è un aspetto importante ma il Titolare è l'organizzazione che decide di raccoglierli e come trattarli.
C. Risposta esatta.
D. Risposta errata. Il Titolare del trattamento è l'organizzazione che ha il potere di decidere quali dati raccogliere e cosa farne. La responsabilità rimane sua anche qualora chieda la consulenza di un esperto.

7. Il Responsabile del trattamento...

❑ A. È il funzionario dell'organizzazione che materialmente si occupa del trattamento dati o ne risponde

❑ B. È l'organizzazione che collabora con il Titolare nel trattamento dei dati

❑ C. È sinonimo di Titolare del trattamento

❑ D. È un esperto che l'organizzazione incarica e che si assume la responsabilità di eventuali inadempienze

A. Non è esatto. Questo valeva con la precedente legislazione. Ora è l'organizzazione che collabora con il Titolare nel trattamento dei dati.
B. Risposta esatta.
C. Non è esatto. Titolare e Responsabile possono coincidere ma è raro. Responsabile è l'organizzazione che collabora con il Titolare nel trattamento dei dati.
D. Non è esatto, questa formula definisce il DPO. Responsabile è l'organizzazione che collabora con il Titolare nel trattamento dei dati.

8. In caso di inadempienza alla norma GDPR...

❑ A. A seconda dei casi risponde il Titolare o il Responsabile

❑ B. È il Responsabile, come dice il nome, che risponde

❑ C. Il Titolare è sempre responsabile

❑ D. Titolare e Responsabile del trattamento sono ambedue responsabili

A. Non è esatto. In linea di principio rispondono ambedue. Poi, analizzando il caso, può essere che la responsabilità sia solo di una delle due organizzazioni.
B. Non è esatto. In linea di principio rispondono ambedue. Poi, analizzando il caso, può essere che la responsabilità sia solo del Responsabile.
C. Non è esatto. In linea di principio rispondono ambedue. Poi, analizzando il caso, può essere che la responsabilità sia solo del Titolare
D. Risposta esatta. A meno che uno dei due non documenti di aver fatto tutto il possibile per impedire che si verificasse il problema sorto o la non aderenza imputata.

9. I rapporti fra Titolare e Responsabile del trattamento...

❑ A. Non devono essere dettagliati: basta definire per iscritto gli ambiti di competenza

❑ B. Devono essere precisati con molta attenzione da un contratto

❑ C. Rapporti di lunga data non hanno bisogno di contrattualizzazione

❑ D. Vanno definiti solo se il Responsabile è un nuovo fornitore del Titolare

A. Non è esatto. Il Titolare ha tutto l'interesse a definire in modo molto dettagliato quali sono i compiti del Responsabile e le garanzie che questi deve prestare.
B. Risposta esatta. Nel contratto o in una serie di documenti o lettere raccomandate.
C. Risposta errata. La durata del rapporto non conta. Il Titolare ha tutto l'interesse a definire in modo dettagliato quali sono i compiti del Responsabile e le garanzie che questi deve prestare.
D. Risposta errata. Vanno definiti con attenzione anche i rapporti pre-esistenti.

10. Se il Responsabile del trattamento ha dei fornitori che collaborano al trattamento dei dati…

❑ A. Il Titolare deve conoscere nome e ruolo di questi subfornitori e ricevere dal Responsabile garanzie scritte

❑ B. Il GDPR non prevede questo caso

❑ C. Non è possibile: i subfornitori devono stringere accordi diretti con il Titolare

❑ D. Sono fatti suoi: il Titolare non deve saperne niente

A. Risposta esatta. Il Titolare deve conoscere tutta la filiera delle aziende che trattano i dati e ricevere – anche tramite il Responsabile – tutte le garanzie necessarie.
B. Al contrario, Il GDPR affronta molto nel dettaglio la cosa, cosciente che nel trattamento dati operano filiere anche molto lunghe di organizzazioni.
C. Questo non è richiesto. Il Titolare deve sapere chi tratterà il dato e ricevere anche indirettamente delle garanzie scritte.
D. Risposta errata. Il Titolare è responsabile in linea di principio di tutto il trattamento dei dati, anche se in parte è effettuato da terzi.

11. Chi decide se l’organizzazione ha il diritto di raccogliere e trattare i dati?

❑ A. L’organizzazione stessa, dopo aver analizzato i rischi, la presenza di un consenso e le misure di sicurezza

❑ B. L’autorità garante della privacy

❑ C. La norma elenca in modo puntiglioso tutti i casi in cui una organizzazione può/non può trattare i dati

❑ D. Il DPO - Data protection officer

A. Risposta esatta. È il concetto di accountability. Il Titolare decide se ha la base giuridica per procedere.
B. Risposta errata. All’Autorità ci si può rivolgere per chiedere un parere, ma non è necessario.
C. Risposta errata. La norma indica una serie di principi e spiega il processo in base al quale il Titolare decide se ha o meno questo diritto o quali misure deve prendere per averlo.
D. Risposta errata. Il DPO è un esperto che può dare il suo parere, ma non è una figura necessaria.

12. Una regola per capire se si ha o meno il diritto di trattare un dato personale è chiedersi…

❑ A. Chi è il Titolare: le organizzazioni senza fine di lucro possono fare tutto, le imprese no

❑ B. Se esistono elenchi precisi di trattamenti ‘proibiti’ e ‘consentiti’

❑ C. Se la persona è in rapporti stretti con l’organizzazione (cliente fedele, aderente, etc.)

❑ D. Se la persona sarebbe sorpresa o poteva essere sorpresa nel sapere di essere oggetto del trattamento

A. Risposta errata. Il GDPR non fa alcuna distinzione fra imprese con e senza fini di lucro.
B. Non è esatto. Questi elenchi non esistono.
C. Risposta errata. Il tipo di rapporto fra l’interessato e il Titolare è rilevante ma non dirimente.
D. Risposta esatta. Questa è la ‘regola del pollice’ più utile per definire la liceità di un trattamento.

13. Un consenso da parte dell’interessato…

❑ A. Non è necessario se il trattamento è funzionale allo svolgimento del servizio richiesto

❑ B. È necessario se si sta operando al fine di massimizzare un profitto o di offrire un miglior servizio

❑ C. È sempre necessario

❑ D. Serve solo se i dati sono trattati da terzi

A. Risposta esatta.
B. Non è esatto. Il fine di lucro in sé non è rilevante e nemmeno il miglioramento del servizio richiesto.
C. Non è esatto. Ci sono situazioni in cui potrebbe non essere necessario.
D. Risposta errata. Il fatto che i dati siano trattati da terzi rende più probabile la necessità di un consenso ma non è questa l’unica situazione.

14. I dati raccolti prima del 25 maggio 2018.

❑ A. Si possono mantenere e trattare senza bisogno di consenso

❑ B. Occorre contattare tutti gli interessati e chiedere loro il consenso

❑ C. Se i dati erano e sono tuttora necessari per eseguire il servizio richiesto, non occorre chiedere il consenso

❑ D. Si possono trattare se l'organizzazione non ha scopo di lucro

A. Risposta errata. Il GDPR non fa alcune distinzione fra i dati raccolti prima o dopo l'entrata in vigore della norma.
B. Non è esatto. Questa è la situazione più frequente ma ci possono essere casi in cui si può fare a meno di richiedere un nuovo consenso e altri in cui basta una notifica con 'silente assenso' da parte dell'interessato.
C. Risposta esatta.
D. Risposta errata. Il GDPR non fa alcuna distinzione fra imprese con e senza fini di lucro.

15. Per raccogliere un consenso valido…
❑ A. Basta fare riferimento alla privacy policy
❑ B. Occorre contattare telefonicamente l'interessato
❑ C. Occorre spiegare le finalità per le quali si richiede il dato, chi lo chiede e come sarà trattato
❑ D. Si possono utilizzare consensi prestati in altre occasioni

A. Non è esatto. Il consenso deve essere contestuale all'Informativa. La lettura delle privacy policy deve essere possibile ma è opzionale.
B. Risposta errata. È sufficiente che il modulo che richiede il consenso contenga l'Informativa.
C. Risposta esatta. È sufficiente che il modulo che richiede il consenso contenga l'Informativa che ha appunto questi contenuti, oltre ad altri minori.
D. Risposta errata. Il consenso prestato per un trattamento non può mai essere utilizzato per altri.

16. L’Informativa all’interessato….

❑ A. Deve essere sempre contestuale al consenso, sintetica ma chiara e contenete le informazioni principali

❑ B. È necessaria solo nel caso di trattamenti complessi

❑ C. Può essere letta dall’interessato in un secondo momento

❑ D. Può essere sostituita dalla privacy policy

A. Risposta esatta: deve chiarire perché sono richiesti questi dati, da chi e come verranno trattati oltre a altri contenuti minori.
B. Risposta errata. Dove è richiesto il consenso ci deve sempre essere l’informativa.
C. Risposta errata. Il consenso deve essere informato e quindi deve discendere dalla lettura dell’informativa.
D. Non è esatto. L’interessato può anche leggere la Privacy policy, che è un documento più esteso, ma l’Informativa deve sempre essere contestuale al consenso.

17. Se alcuni dei dati richiesti sono soggetti a un trattamento diverso…

❑ A. Occorrono diversi moduli di consenso

❑ B. Ogni dato chiesto va giustificato e deve essere possibile prestare consenso all'utilizzo di alcuni dati e non di altri

❑ C. Il consenso riguarda sempre tutti i dati presenti nel modulo

❑ D. Una volta prestato il consenso, il dato può essere trattato in ogni modo

A. Non è esatto. Può bastare lo stesso modulo ma se alcuni dati hanno trattamenti diversi deve essere possibile per l'interessato consentire solo al trattamento di alcuni.
B. Risposta esatta.
C. Risposta errata. Se alcuni dati hanno trattamenti diversi, deve essere possibile per l'interessato consentire al trattamento di alcuni e non di altri.
D. Risposta errata. Se alcuni dati hanno trattamenti diversi deve essere possibile per l'interessato consentire al trattamenti di alcuni e non di altri.

18. La revoca del consenso.

❑ A. Coincide con la cancellazione di tutti i dati relativi all'interessato

❑ B. Deve essere una procedura semplice come la sua concessione e può riferirsi solo a specifici trattamenti

❑ C. Non può mai avvenire

❑ D. Può avvenire solo se la richiesta giunge via raccomandata o PEC

A. Non è esatto. Si può revocare il consenso solo ad alcuni trattamenti o al trattamento di alcuni dati.
B. Risposta esatta.
C. Risposta errata. Il consenso deve sempre essere revocabile.
D. Risposta errata. Il consenso deve sempre essere revocabile con qualunque mezzo, e sicuramente con il mezzo utilizzato per prestarlo.

19. Privacy policy.

❑ A. La privacy policy deve essere sempre disponibile ma può essere solo riassunta nell'informativa

❑ B. La privacy policy è necessaria solo se i dati sono trattati da terzi

❑ C. La privacy policy è richiesta solo alle aziende con oltre 250 dipendenti

❑ D. Prima di prestare un consenso è necessario che l'interessato legga la privacy policy

A. Risposta esatta.
B. Non è esatto. La norma non impone la presenza di una privacy policy ma la consiglia in tutti i casi.
C. Non è esatto. La norma non fa alcuna distinzione relativa alla dimensione dell'impresa.
D. Non è esatto. L'interessato può anche leggere la privacy policy, che è un documento più esteso, ma può bastare la lettura dell'Informativa.

20. I dati forniti dall’interessato...

❑ A. Devono essere cancellati comunque entro un anno

❑ B. Devono essere cancellati non appena è terminata la transazione che li ha richiesti

❑ C. Possono essere mantenuti e trattati indefinitamente

❑ D. Se non sono necessari, devono essere cancellati dopo un ragionevole periodo di tempo

A. Non è esatto. La norma consiglia di non mantenere i dati per un tempo inutilmente lungo ma non pone limiti temporali assoluti.
B. Non è esatto. La norma consiglia di non mantenere i dati per un tempo inutilmente lungo ma non pone limiti temporali assoluti.
C. Risposta errata. La norma richiede di stabilire un termine.
D. Risposta esatta.

21. I dati presenti nei cookie…

❑ A. Non rappresentano un dato personale oggetto del GDPR

❑ B. Sono anonimi e non permettono di identificare l'interessato

❑ C. Sono sempre cancellati non appena l'interessato spegne il computer

❑ D. Sono un dato personale in quanto potrebbero identificare l'interessato o fornire informazioni su di lui

A. Risposta errata. Il GDPR, al contrario, tratta in modo specifico i Cookie.
B. Non è esatto. Attraverso i cookie e incrociando i dati raccolti nelle navigazioni dell'interessato è possibile raccogliere molte informazioni e perfino identificare in modo preciso l'interessato.
C. Non è esatto. I cookie di sessione sono cancellati, ma la maggioranza dei cookie rimane.
D. Risposta esatta.

22. Quali di questi dati non sono considerati sensibili?

❑ A. Immagini e video che ritraggono l'interessato

❑ B. Informazioni relative agli orientamenti sessuali, filosofici o religiosi

❑ C. Informazioni relative alla salute

❑ D. Informazioni su condanne o citazioni in giudizio dell'interessato

A. Risposta esatta. Immagini e video non sono automaticamente considerati dati sensibili.
B. Risposta errata. Queste informazioni sono considerate sensibili e quindi soggette a particolari attenzioni e restrizioni di trattamento.
C. Risposta errata. Queste informazioni sono considerate sensibili e quindi soggette a particolari attenzioni e restrizioni di trattamento.
D. Risposta errata. Queste informazioni sono considerate sensibili e quindi soggette a particolari attenzioni e restrizioni di trattamento.

23. Se un trattamento riguarda dati sensibili...

❑ A. È proibito se il dato è raccolto dopo il 25 maggio 2018

❑ B. È sempre proibito

❑ C. Potrebbe essere svolto ma richiede un consenso, una solida base giuridica e particolari attenzioni

❑ D. Può essere svolto da qualunque organizzazione purché senza finalità commerciali

A. Risposta errata. La norma non fa alcuna distinzione fra i dati raccolti prima e dopo l'entrata in vigore o l'inizio dell'efficacia del GDPR.
B. Non è esatto. Sicuramente il Titolare deve avere solide basi giuridiche per poterli trattare e deve avere messo in atto misure di sicurezza particolarmente solide.
C. Risposta esatta.
D. Risposta errata. La norma non fa alcuna distinzione fra le finalità commerciali e non commerciali del trattamento.

24. L’interessato ha diritto a conoscere, a rettificare o a cancellare i dati che lo riguardano.

❑ A. Sempre e comunque in modo semplice e potendo contare su una rapida esecuzione

❑ B. Solo dietro richiesta dell’Autorità giudiziaria

❑ C. Solo se fa domanda alla Autorità Garante della Privacy

❑ D. Solo se il dato è stato raccolto senza il suo consenso

A. Risposta esatta.
B. Risposta errata. L’autorità giudiziaria non c’entra nulla. L’interessato è proprietario del dato e può chiedere in ogni momento queste attività.
C. Risposta errata. L’Autorità garante non c’entra nulla. L’interessato è proprietario del dato e può chiedere in ogni momento queste attività.
D. Non è esatto. Prestare il consenso al trattamento non annulla il diritto a chiederne la rettifica o la cancellazione.

25. Nei computer e nei server che li contengono, i dati personali in possesso dell'organizzazione devono essere accessibili.

❑ A. Solo da persone autorizzate senza bisogno di una password

❑ B. Solo da persone autorizzate alle quali viene rivelata la password valida per tutti

❑ C. Solo da persone autorizzate in possesso di una password personale 'sicura' cambiata di frequente

❑ D. Solo da persone autorizzate in possesso di una password qualsiasi, per esempio quella della loro mail

A. Risposta errata. Per garantire la necessaria sicurezza è necessario che ai dati possano accedere solo le persone che hanno una password personale sicura e cambiata di frequente.
B. Risposta errata. Per garantire la necessaria sicurezza è necessario che ai dati possano accedere solo le persone che hanno una password personale sicura e cambiata di frequente.
C. Risposta esatta.
D. Risposta errata. Per garantire la necessaria sicurezza è necessario che ai dati possano accedere solo le persone che hanno una password personale sicura e cambiata di frequente.

26. Quale di queste password è preferibile utilizzare?

- ❑ A. Data di nascita del primo figlio
- ❑ B. Frase di una poesia o un libro o una canzone
- ❑ C. Nome del proprio cane o del gatto
- ❑ D. Proprio nome di battesimo+anno di nascita

A. Risposta errata. È un dato relativamente facile da ottenere e quindi sconsigliabile.
B. Risposta esatta. Le password lunghe sono più difficilmente intuibili. Meglio ancora se prevedono anche un numero. Esempio: 44gattiinfilaper6colrestodi2.
C. Risposta errata. È un dato relativamente facile da ottenere (pensiamo alle foto che mettiamo sui social media) e quindi sconsigliabile.
D. Risposta errata. È un dato relativamente facile da ottenere e quindi sconsigliabile.

27. Sistemi operativi e programmi antivirus…

❑ A. Meglio non aggiornarli perché le nuove versioni rallentano il computer

❑ B. Meglio tenere le versioni vecchie e più sicure

❑ C. Vanno comprati quando si acquista un computer nuovo

❑ D. Vanno sempre aggiornati per prevenire virus e attacchi informatici

A. Non è esatto. È vero che rallentano il computer ma la sicurezza è ancora più importante.
B. Risposta errata. Le versioni nuove hanno corretto le falle che nelle precedenti versioni consentivano accessi non autorizzati. Quindi vanno sempre aggiornati all'ultima versione esistente.
C. Risposta errata. Le versioni nuove hanno corretto le falle che nelle precedenti versioni consentivano accessi non autorizzati. Quindi vanno sempre aggiornati all'ultima versione esistente.
D. Risposta esatta.

28. Il cloud computing.

❑ A. È il nome tecnico della trasmissione dati da/per smartphone

❑ B. È la soluzione consigliata dal GDPR per la gestione dei dati raccolti su web

❑ C. È una modalità di elaborazione e gestione dei dati che rende difficile sapere dove si trovino fisicamente

❑ D. Trattandosi di una tecnologia recente, non è considerata dal GDPR

A. Risposta errata. Si parla di cloud computing quando dati e applicazioni non risiedono in una locazione fisica nota ma possono essere dislocati in più server, potenzialmente anche al di fuori dell'Unione Europea.
B. Risposta errata. Si parla di cloud computing quando dati e applicazioni non risiedono in una locazione fisica nota ma possono essere dislocati in più server, potenzialmente anche al di fuori dell'Unione Europea.
C. Risposta esatta.
D. Risposta errata. Al contrario il GDPR parla diffusamente della questione.

29. Il Data protection officer.

❑ A. È il titolo assegnato in ogni organizzazione alla persona che si occupa dei dati

❑ B. È un altro nome del Responsabile del trattamento

❑ C. È un altro nome del Titolare del trattamento

❑ D. È un professionista, interno o esterno all'organizzazione, necessario in determinati casi

A. Risposta errata: È un professionista interno o esterno all'organizzazione necessario in determinati casi.
B. Risposta errata: È un professionista interno o esterno all'organizzazione necessario in determinati casi.
C. Risposta errata: È un professionista interno o esterno all'organizzazione necessario in determinati casi.
D. Risposta esatta.

30. In conclusione: il modo migliore per adeguarsi al GDPR è:

❑ A. Attendere che le cose si siano chiarite e poi copiare quello che fanno gli altri

❑ B. Chiamare un esperto e affidare a lui tutto

❑ C. Documentare ogni aspetto della attività propria e dei fornitori che abbia a che fare con i dati personali

❑ D. Sperare che non succeda nulla e fare quel che si è sempre fatto

A. Non è esatto. Potrebbero passare diversi mesi o anni nel corso del quali il Titolare potrebbe essere soggetto a sanzioni anche pesanti. Poi ogni situazione è diversa dalle altre e il 'copia e incolla' in questi casi non funziona.
B. Non è esatto. Un esperto può aiutare ma non sempre è necessario e comunque non è possibile delegargli la responsabilità.
C. Risposta esatta.
D. Risposta errata. È molto facile scoprire anche dall'esterno (pensiamo ai siti web) se una azienda non rispetta il GDPR.