

GDPR - EU General Data Protection Regulation
Regolamento Europeo 2016/679
in materia di protezione dei dati personali

GDPR

Politica e obiettivi

Titolare del trattamento

KENT SERVICE
VIA A. MORO 109
SAN DONATO
MIL.SE



Sommario

1. Politica e obiettivi	3
ARTICOLI DEL REGOLAMENTO	5
2. I principi fondamentali del Regolamento Privacy.....	10
3. I diritti dell'interessato previsti dal regolamento privacy.....	12
4. Il sistema organizzativo del regolamento europeo privacy	15
5. Gli adempimenti del regolamento privacy europeo	16
Informativa.....	27
Consenso.....	28



1. Politica e obiettivi

Il nuovo Regolamento europeo sulla protezione dei dati introduce un'unica legislazione in tutte e 28 le nazioni dell'UE.. Le aziende devono adeguarsi alle nuove disposizioni, non solo per evitare pesanti sanzioni, ma anche per essere più competitive in un mercato unico digitale.

Per le aziende e i professionisti, di qualsiasi ordine e grado, cambia radicalmente la visione generale che passa da un censimento dei trattamenti effettuati relativi alla privacy ad un vero e proprio Sistema Rischi.

La nostra azienda, nel recepire il Regolamento, si pone l'obiettivo di soddisfare le misure organizzative e tecniche per la protezione dei dati personali.

Considerata la complessità dell'argomento, il percorso organizzativo e tecnico è oggetto di un costante aggiornamento nel tempo.

Viene evidenziato il fatto che la politica e le tecniche di protezione dei dati sono rivolte a tutte le attività di trattamento dei dati e applicate a tutti i dati personali gestiti, ovviamente modulate a seconda della tipologia dei dati e del trattamento loro riservato.

Il trattamento dei dati personali contempla anche il fatto che tali dati possono essere trasferiti a soggetti terzi ai quali viene richiesta la documentazione a garanzia della corretta gestione secondo la normativa in essere.

La documentazione prodotta a sostegno della conformità al Regolamento viene periodicamente aggiornata in concomitanza con i miglioramenti che verranno introdotti nel tempo relativi alle misure di tutele dei dati personali e, se del caso, in virtù di eventuali novità normative.



Sono state recepite le modifiche e integrazioni rispetto al Codice Privacy, in particolare:

- Informativa art. 13
- Consenso art. 6
- Misure di sicurezza adeguate art. 32
- Nomina DPO art. 37
- Valutazione d'impatto art. 35
- Consultazione preventiva art. 36
- Privacy by design/default art. 25
- Registro dei trattamenti art. 30
- Certificazione art. 25 - 42
- Violazione dati (data breach) art. 33 - 34
- Trasferimento dati all'estero art. 44
- Diritto di accesso dell'interessato art. 15
- Diritto di rettifica art. 16
- Diritto alla cancellazione («diritto all'oblio») art. 17

Il Registro dei trattamenti evidenzia in dettaglio:

- L'organigramma aziendale
- La distribuzione dei compiti e delle responsabilità
- Il trattamento dei dati personali
- La gestione degli incaricati del trattamento
- L'elenco delle apparecchiature installate
- Gli amministratori di sistema
- L'analisi dei rischi e le misure di sicurezza

ARTICOLI DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

Articolo 1. Oggetto e finalità	Articolo 48. Trasferimento o comunicazione non autorizzati dal diritto dell'Unione
Articolo 2. Ambito di applicazione materiale	Articolo 49. Deroghe in specifiche situazioni
Articolo 3. Ambito di applicazione territoriale	Articolo 50. Cooperazione internazionale per la protezione dei dati personali
Articolo 4. Definizioni	Articolo 51. Autorità di controllo
Articolo 5. Principi applicabili al trattamento dei dati personali	Articolo 52. Indipendenza
Articolo 6. Liceità del trattamento	Articolo 53. Condizioni generali per i membri dell'Autorità di controllo
Articolo 7. Condizioni per il consenso	Articolo 54. Norme sull'istituzione dell'Autorità di controllo
Articolo 8. Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione	Articolo 55. Competenza
Articolo 9. Trattamento di categorie particolari di dati personali	Articolo 56. Competenza dell'Autorità di controllo capofila
Articolo 10. Trattamento dei dati personali relativi a condanne penali e reati	Articolo 57. Compiti
Articolo 11. Trattamento che non richiede l'identificazione.	Articolo 58. Poteri
Articolo 12. Trasparenza e modalità	Articolo 59. Relazioni di attività
Articolo 13. Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato	Articolo 60. Cooperazione tra l'Autorità di controllo capofila e le altre Autorità di controllo
Articolo 14. Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato	Articolo 61. Assistenza reciproca
Articolo 15. Diritto di accesso dell'interessato	Articolo 62. Operazioni congiunte delle Autorità di controllo
Articolo 16. Diritto di rettifica	Articolo 63. Meccanismo di coerenza
Articolo 17. Diritto alla cancellazione («diritto all'oblio»)	Articolo 64. Parere del comitato europeo per la protezione dei dati
Articolo 18. Diritto di limitazione di trattamento	Articolo 65. Composizione delle controversie da parte del comitato
Articolo 19. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento	Articolo 66. Procedura d'urgenza
Articolo 20. Diritto alla portabilità dei dati	Articolo 67. Scambio di informazioni
Articolo 21. Diritto di opposizione	Articolo 68. Comitato europeo per la protezione dei dati
Articolo 22. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione	Articolo 69. Indipendenza
Articolo 23. Limitazioni	Articolo 70. Compiti del comitato
Articolo 24. Responsabilità del Titolare del trattamento	Articolo 71. Relazioni
Articolo 25. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita	Articolo 72. Procedura
Articolo 26. Contitolari del trattamento	Articolo 73. Presidente
Articolo 27. Rappresentanti di Titolari del trattamento o dei Responsabili del trattamento non stabiliti nell'Unione	Articolo 74. Compiti del presidente
Articolo 28. Responsabile del trattamento	Articolo 75. Segreteria
Articolo 29. Trattamento sotto l'Autorità del Titolare del trattamento o del Responsabile del trattamento	Articolo 76. Riservatezza
Articolo 30. Registri delle attività di trattamento	Articolo 77. Diritto di proporre reclamo all'Autorità di controllo
Articolo 31. Cooperazione con l'Autorità di controllo	Articolo 78. Diritto a un ricorso giurisdizionale effettivo nei confronti dell'Autorità di controllo
Articolo 32. Sicurezza del trattamento	Articolo 79. Diritto a un ricorso giurisdizionale effettivo nei confronti del Titolare del trattamento o del Responsabile del trattamento
Articolo 33. Notifica di una violazione dei dati personali	Articolo 80. Rappresentanza degli interessati
Articolo 34. Comunicazione di una violazione dei dati personali all'interessato	Articolo 81. Sospensione delle azioni
Articolo 35. Valutazione d'impatto sulla protezione dei dati all'Autorità di controllo	Articolo 82. Diritto al risarcimento e responsabilità
Articolo 36. Consultazione preventiva	Articolo 83. Condizioni generali per infliggere sanzioni amministrative pecuniarie
Articolo 37. Designazione del Responsabile della protezione dei dati	Articolo 84. Sanzioni
Articolo 38. Posizione del Responsabile della protezione dei dati	Articolo 85. Trattamento e libertà d'espressione e di informazione
Articolo 39. Compiti del Responsabile della protezione dei dati	Articolo 86. Trattamento e accesso del pubblico ai documenti ufficiali
Articolo 40. Codici di condotta	Articolo 87. Trattamento del numero di identificazione nazionale
Articolo 41. Monitoraggio dei codici di condotta approvati	Articolo 88. Trattamento dei dati nell'ambito dei rapporti di lavoro
Articolo 42. Certificazione	Articolo 89. Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse,
Articolo 43. Organismi di certificazione	Articolo 90. Obblighi di segretezza
Articolo 44. Principio generale per il trasferimento	Articolo 91. Norme di protezione dei dati vigenti presso chiese e associazioni religiose
Articolo 45. Trasferimento sulla base di una decisione di adeguatezza	Articolo 92. Esercizio della delega
Articolo 46. Trasferimento soggetto a garanzie adeguate	Articolo 93. Procedura di comitato
Articolo 47. Norme vincolanti d'impresa	Articolo 94. Abrogazione della direttiva 95/46/CE
	Articolo 95. Rapporto con la direttiva 2002/58/CE
	Articolo 96. Rapporto con accordi precedentemente conclusi
	Articolo 97. Relazioni della Commissione
	Articolo 98. Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati
	Articolo 99. Entrata in vigore e applicazione

Vengono di seguito riportati gli estratti dei 99 articoli del Regolamento indicando quanto viene fatto per ciascun articolo che presenta un diretto riferimento con quanto si mette in atto per essere conformi.

Art. 1. Oggetto e finalità

Il presente Regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

Il presente Regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

I dati personali presi in esame sono solo quelli relativi a persone fisiche, il Regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche.

Il Regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico (es. uso dei social network, corrispondenza, indirizzari) e, quindi, senza una connessione con un'attività commerciale o professionale.

Vengono trattati dati relativi a persone fisiche e a persone giuridiche, queste ultime non sono disciplinate dal Regolamento

Art. 2. Ambito di applicazione materiale

Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Non si eseguono trattamenti automatizzati

Art. 3 Ambito di applicazione territoriale

Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

I trattamenti sono eseguiti nell'ambito dell'Unione

Art. 4. Definizioni

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

Non si eseguono attività di profilazione

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Il ricorso, da parte del Titolare, alla pseudonimizzazione e alla crittografia non deve avvenire di default ma nei soli casi in cui egli – valutati i rischi legati al trattamento dei dati che si intende porre in essere reputi necessario ricorrere ad essi.

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; es. di archivi sono: cartelle cliniche, elenco clienti, elenco fornitori, elenco dipendenti, ecc.

7) «Titolare del trattamento»: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «Responsabile del trattamento»: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

Non si è reputato necessario nominare un Responsabile del trattamento la cui designazione è facoltativa

9) «destinatario»: la persona fisica o giuridica, l'Autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le Autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette Autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web). Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito». Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi.

L'informativa e il consenso vengono gestiti in conformità con il Regolamento

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

il Garante per la protezione dei dati personali ha adottato negli ultimi anni una serie di provvedimenti che introducono in determinati settori l'obbligo di comunicare eventuali violazioni di dati personali (data breach) all'Autorità stessa e, in alcuni casi, anche ai soggetti interessati. Il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni amministrative.

Nel caso di violazioni di dati personali che sono stati preventivamente criptati non c'è obbligo di notifica dell'eventuale data breach al Garante; in caso contrario la notifica deve essere fatta entro 72 ore dall'avvenimento del fatto, con una sorta di autodenucia.

Si dovrebbe sostenere un costo elevato per realizzare la criptazione dei dati, considerato il basso rischio di intrusione non si reputa necessario adottare tale tecnica.

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

Non vengono gestiti dati genetici

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici ;

Non vengono gestiti dati biometrici

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a) per quanto riguarda un Titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del Titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un Responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il Responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del Responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del Responsabile del trattamento nella misura in cui tale Responsabile è soggetto a obblighi specifici ai sensi del presente Regolamento;

Il Responsabile del trattamento non è stato nominato essendo la nomina facoltativa.

Art. 29. Responsabile del trattamento.

Il responsabile è designato dal titolare facoltativamente.

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal Titolare del trattamento o dal Responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente Regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un Titolare del trattamento o Responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un Titolare del trattamento o Responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

2. I principi fondamentali del Regolamento Privacy

Art. 5 Principi applicabili al trattamento dei dati personali

1. I dati personali sono:

- a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente Regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il Titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («Responsabilizzazione»).

Si effettua il trattamento dei dati in conformità all' Art. 5

Art. 6 Liceità del trattamento

Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;

Base giuridica del trattamento: (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Se il trattamento avviene per un fine diverso da quello per il quale si è acquisito il consenso occorre verificare:

- a) l'esistenza di un eventuale nesso tra la finalità di trattamento per la quale si è acquisito il consenso e la nuova finalità;
- b) la relazione esistente tra il Titolare e l'interessato;
- c) la natura dei dati personali trattati;
- d) le conseguenze che potrebbero derivare, in capo all'interessato, dal nuovo trattamento;
- e) la presenza di misure atte ad impedire la identificazione dell'interessato (cifatura o pseudonimizzazione).

Si esegue il trattamento dei dati in base alle condizioni che sono alla base del principio di liceità , in particolare: consenso quando necessario, esecuzione di un contratto, obblighi di legge.

Art. 7 Condizioni per il consenso

Qualora il trattamento sia basato sul consenso, il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Quando il consenso è necessario viene conservata la documentazione relativa all'ottenimento.

Art. 8. Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione.

Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli eventuali trattamenti relativi ai minori sono effettuati dopo aver avuto il consenso dal titolare della responsabilità genitoriale.

Articolo 9 Trattamento di categorie particolari di dati personali

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

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

I dati particolari vengono trattati in conformità dell'articolo 9

3. I diritti dell'interessato previsti dal regolamento privacy

Art. 12. Trasparenza e modalità

Il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici.

Articolo 13.

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

In caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

- a) l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del Responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

Articolo 14.

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.

Qualora i dati non siano stati ottenuti presso l'interessato, il Titolare del trattamento fornisce all'interessato le seguenti informazioni:

- a) l'identità e i dati di contatto del Titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del Responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) le categorie di dati personali in questione;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o ad un'organizzazione internazionale

Articolo 15 Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano od opporsi al loro trattamento;
- f) il diritto di proporre reclamo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni sulla loro origine,
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

LA PRESENTE AZIENDA, ALLO STATO, NON ADOTTA PROCESSI AUTOMATIZZATI NE' LA PROFILAZIONE

Articolo 16. Diritto di rettifica

L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 17 Diritto alla cancellazione («diritto all'oblio»)

L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento;
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Quanto sopra non è applicabile nella misura in cui il trattamento sia necessario.

Articolo 18 Diritto di limitazione di trattamento

L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benchè il titolare del trattamento non ne abbia più bisogno al fine del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d) l'interessato si è opposto al trattamento ai sensi dell'art. 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Articolo 19.

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento.

Il Titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1 e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 20 Diritto alla portabilità dei dati

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti.

Articolo 21 Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento per motivi connessi alla sua situazione, al trattamento dei dati personali che lo riguardano, compresa la profilazione, anche per finalità di marketing diretto e di tale opportunità deve essere data continua comunicazione in ogni successivo messaggio a scopo di commercializzazione. La comunicazione volta all'interruzione del trattamento per tali finalità deve, inoltre, essere gratuita, ad eccezione degli eventuali costi relativi alla trasmissione. Sempre salvo che il titolare dimostri l'esistenza ma di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria e salvo che il trattamento dia necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 22 Processo decisionale automatizzato relativo alle persone fisiche

L'interessato ha diritto a non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Le regole varate armonizzano e rendono più chiara la gestione delle attività di profilazione, ovvero la definizione di "profili" di utenti (sulla base di caratteristiche, comportamenti, scelte, abitudini) allo scopo di fornire servizi o promozioni personalizzate. Dovranno essere adottate da tutti i soggetti stabiliti su territorio nazionale che forniscono servizi on line, quali motori di ricerca, posta elettronica, mappe online, social network, pagamenti elettronici, cloud computing.

Ecco in sintesi le regole previste nelle Linee guida:

Informativa

L'informativa sul trattamento dei dati dovrà essere chiara, completa, esaustiva e resa ben visibile, già dalla prima pagina del sito. Essa costituisce il presupposto per consentire agli interessati medesimi di esprimere o meno il consenso all'uso dei propri dati per fini di profilazione ed è preferibile che sia strutturata su più livelli, per renderne più facile la lettura: un primo livello immediatamente accessibile con un solo click dalla pagina visitata, con tutte le informazioni di maggiore importanza (ad esempio l'indicazione dei trattamenti e dei dati oggetto di trattamento); un secondo livello, accessibile dal primo, con ulteriori dettagli sui servizi offerti.

Consenso

Qualunque attività di trattamento dei dati personali dell'utente per finalità di profilazione e diversa da quelle necessarie per la fornitura del servizio (ad esempio, i filtri antispam o antivirus, gli strumenti per consentire ricerche testuali, etc.) potrà essere effettuata esclusivamente con il consenso informato dell'utente. Questo obbligo si applica dunque alla profilazione per finalità promozionali comunque effettuata: sia quella sui dati relativi all'uso della posta elettronica, sia quella basata sull'incrocio dei dati personali raccolti in relazione all'utilizzo di più funzionalità da parte degli utenti (ad esempio: posta elettronica e navigazione sul web, partecipazione a social network e utilizzo di mappe o visualizzazione di contenuti).

Tutele per ogni utente

Le società dovranno tutelare la privacy sia degli utenti autenticati, cioè quelli che accedono ai servizi tramite un account (ad esempio per l'utilizzo della posta elettronica), sia di quelli che fanno uso dei servizi in assenza di previa autenticazione (utenti non autenticati), come in caso di semplice navigazione on line audiovisivi etc., sia infine quella fondata sull'impiego di strumenti di identificazione diversi dai cookie (come il fingerprinting, che costruisce profili dell'utente sulla base di specifici parametri di impostazione del terminale o sulle modalità del suo utilizzo).

Attraverso modalità semplificate, gli utenti potranno scegliere in modo attivo e consapevole se acconsentire alla profilazione. All'utente dovrà comunque essere sempre pienamente garantito il diritto di revoca delle scelte espresse in precedenza. A tale scopo dovrà essere predisposto un link, sempre ben visibile.

Articolo 23 Limitazioni

Il diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o il Responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti per salvaguardare la sicurezza nazionale, la difesa e la sicurezza pubblica oltre che per la prevenzione, l'indagine, l'accertamento ed il perseguimento di reati od altri importanti obiettivi di interesse pubblico.

4. Il sistema organizzativo del regolamento europeo privacy

Articolo 24 Responsabilità del Titolare del trattamento

In capo al Titolare del trattamento sono previsti gli obblighi relativi alla predisposizione delle misure tecniche ed organizzative "adeguate" per rispondere a due requisiti, essere in grado di:

a) garantire l'applicazione delle prescrizioni contenute nel Regolamento

b) dimostrare, se richiesto, di essersi attivati in tale direzione (accountability). Va precisato che, a differenza di quanto stabilito dalla Direttiva 95/46/CE la quale introduceva una distinzione tra misure di sicurezza minime ed idonee, l'applicazione di misure di sicurezza è finalizzata alla messa in sicurezza della organizzazione: ciò significa che la conformità non garantisce la sicurezza mentre è vero il contrario, cioè che la sicurezza rende compliance le misure predisposte.

L'adozione di misure tecniche ed organizzative deve avvenire all'interno di un processo di miglioramento continuo, il che comporta in capo al Titolare l'obbligo di intervenire ogni qual volta ciò si renda necessario (ad es. perché è cambiata la normativa oppure perché sono intervenute nuove tecnologie che vanno ad impattare sui trattamenti in essere, oppure, ancora, perché si implementano nuovi trattamenti).

Articolo 25

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'approccio alla Privacy by Design (fin dalla progettazione) è caratterizzato da interventi di tipo proattivo e non reattivo. Esso anticipa e previene le violazioni della privacy prima che essi accadano.

La privacy by default (per impostazione predefinita) presuppone invece, nella modalità operativa del trattamento, misure e tecniche che, per impostazione predefinita, garantiscano l'utilizzo dei soli dati personali necessari per ciascuna specifica finalità di trattamento; e che la quantità dei dati e la durata della loro conservazione non eccedano i tempi minimi necessari per il raggiungimento delle finalità perseguire.

Adempimenti in capo al Titolare del trattamento

1. Predisposizione di informative e consensi idonei per i servizi rilasciati on line;
2. Valutazione di data transfer agreement per i dati inviati per il trattamento verso Paesi extra UE;
3. Anonimizzazione dei dati o predisposizione di codici identificativi per la creazione e gestione di banche dati (DB) con dati sulla salute;
4. Predisposizione di regole sulla conservazione dei dati e sulla cancellazione sicura degli stessi;
5. Valutazione della reale conservazione di immagini nei termini di legge per gli impianti di videosorveglianza;
6. Creazione di user e password univoche e non di gruppo per trattamento dati (DB);
7. Aggiornamento della notifica all'Autorità Garante per la protezione dei dati.

Il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità di trattamento

Articolo 26. Contitolari del trattamento

Nell'organigramma privacy si introduce la figura del contitolare del trattamento allorché due o più Titolari condividono, congiuntamente, le finalità ed i mezzi del trattamento. Ricorrendo tale caso si procede ad una definizione dei relativi ambiti di competenza, attraverso la redazione di un accordo interno, che va ad esplicitare da chi vengono rispettate le regole contenute nel Regolamento e chi deve riscontrare le istanze del soggetto interessato del trattamento.

Articolo 27. Rappresentanti di Titolari del trattamento o dei Responsabili del trattamento non stabiliti nell'Unione

Ove titolare del trattamento risulti essere un soggetto stabilito in un Paese non appartenente all'unione europea, questi, a norma dell'art. 2, comma 1 ter della legge n. 675/1996, è tenuto a designare un rappresentante stabilito nel territorio dello Stato.

Articolo 28. Responsabile del trattamento

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

Articolo 29. Trattamento sotto l'Autorità del Titolare del trattamento o del Responsabile del trattamento

Il Responsabile del trattamento, o chiunque agisca sotto la sua Autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

5. Gli adempimenti del regolamento privacy europeo

L'Analisi dei Rischi Privacy

L'analisi dei rischi viene descritta nel *Registro dei trattamenti*

La Valutazione dell'Impatto sulla Protezione dei Dati Personali

La valutazione d'impatto potrebbe anche non essere redatta in quanto non vengono effettuati trattamenti automatizzati e neppure sorveglianza sistematica su larga scala.

Le Misure di Sicurezza

Le misure di sicurezza adottate sono descritte nel *Registro dei trattamenti*

Il Trasferimento dei Dati all'Estero

La Società, per l'attività che le è propria, può trasferire dati personali all'estero.

La Notifica delle Violazioni dei Dati Personali (data breach)

La notifica delle violazioni dei dati personali ricade sul Titolare del trattamento e deve essere comunicata all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

E' stata adottata la modulistica e la modalità per comunicare l'eventuale violazione dei dati nei tempi e metodi previsti dal Regolamento.

Articolo 30 Registri delle attività di trattamento

Ogni Titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria Responsabilità contenente il nome ed i dati di contatto del titolare del trattamento. E del responsabile della protezione dati, le finalità del trattamento, la descrizione delle categorie di interessati e delle categorie di dati personali trattati nonché le categorie dei destinatari a cui i dati verranno comunicati, in trasferimenti dei dati personale, ove possibile, i termini ultimi per la cancellazione delle diverse categorie dei dati.

I suddetti Registri non sono obbligatori per i Titolari con meno di 250 dipendenti, salvo che il trattamento non comprenda dati sensibili, il trattamento non sia occasionale o non sia presente un rischio per i diritti e le libertà dell'interessato.

Viene tenuto il Registro dei Trattamenti

Articolo 31 Cooperazione con l'Autorità di controllo

Il Titolare del trattamento, il Responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti. È imposto in capo al Titolare, al Responsabile ed al rappresentante l'obbligo di cooperare con l'Autorità di controllo che agisce nella esecuzione dei propri compiti. Per cui le saranno fornite, a seguito di richiesta, informazioni e documenti e sarà agevolata la sua, eventuale, attività di indagine e controllo.

La cooperazione con l'autorità di controllo viene recepita e garantita dalla Società.

Articolo 32. Sicurezza del trattamento

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del trattamento e il Responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio come la pseudonomizzazione e la cifratura dei dati personali, la capacità di assicurare riservatezza, integrità, disponibilità e resilienza dei sistemi, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali nel caso di incidente, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

Con il Regolamento, cambia la prospettiva per le misure di sicurezza: non c'è più distinzione tra misure minime e idonee; le prime erano dettagliatamente individuate dal legislatore agli artt. 33-34 e all'Allegato B del Codice stesso (d.lgs. n. 196/2003), mentre le seconde dovevano essere determinate dal Titolare del trattamento alla luce di una serie di parametri a cui fare riferimento, che andavano dalla tipologia di dati trattati alla modalità di trattamento e dalla quantità di dati trattati alla loro trasferibilità al di fuori della UE, ecc..

In base al Regolamento, esistono solo misure adeguate da applicare, decise dal Titolare del trattamento a seguito dell'analisi dei rischi.

Le misure di sicurezza sono state adottate e sono suscettibili di continui miglioramenti nel tempo anche in considerazione dello sviluppo tecnologico e delle necessità rispetto alla tipologia di trattamento ed all'analisi dei rischi. Le misure di sicurezza sono riportate in dettaglio nel Registro dei trattamenti.

Articolo 33. Notifica di una violazione dei dati personali all'Autorità di controllo

In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Ovviamente, tra le altre cose, dovrà essere comunicata la natura della violazione, il numero e le categorie di interessati dalla violazione, il nome del responsabile della protezione dei dati oltre che le probabili conseguenze e le misure adottate o di cui si propone l'adozione.

Articolo 34. Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

Articolo 35. Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento effettua, prima di procedere al trattamento una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nel caso di:

1. 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 sugli interessati;
2. trattamento, su larga scala, di categorie particolari di dati personali (sensibili o giudiziari);
3. sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Articolo 36. Consultazione preventiva

Il Titolare del trattamento, prima di procedere al trattamento, consulta l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio.

Articolo 37. Designazione del Responsabile della protezione dei dati - Data Protection Officer (D.P.O.)

Il Titolare del trattamento e il Responsabile del trattamento designano sistematicamente un Responsabile della protezione dei dati ogniqualvolta: 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 del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure 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'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Differenza tra il D.P.O. ed il Responsabile del trattamento dei dati personali.

Alla luce dei requisiti e dei compiti attribuiti alle due figure sopra menzionate: mentre il primo deve essere indipendente ed autonomo, il secondo deve agire seguendo solo e soltanto le istruzioni del titolare del trattamento: pertanto ha un vincolo che gli impedisce di godere di ampia indipendenza, tipica invece del ruolo del DPO.

Non si rientra nei casi per i quali viene richiesta la figura del Responsabile della protezione dei dati - Data Protection Officer (D.P.O.)

Articolo 38. Posizione del Responsabile della protezione dei dati

Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

Non si rientra nei casi per i quali viene richiesta la figura del Responsabile della protezione dei dati - Data Protection Officer (D.P.O.)

Articolo 39. Compiti del Responsabile della protezione dei dati

Il Responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati; b) sorvegliare l'osservanza del presente Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle Responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo; c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35; d) cooperare con l'Autorità di controllo; e e) fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Articolo 40. Codici di condotta

Gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri.

L'aspetto maggiormente considerato consiste nell'accertare la presenza, in detti codici, dei principi base della normativa di settore, quali:

- a) la qualità e la proporzionalità dei dati,
- b) la trasparenza,
- c) la sicurezza,
- d) i diritti di accesso, rettifica e opposizione,
- e) l'esigenza di una tutela rafforzata per i dati sensibili.

Articolo 41. Monitoraggio dei codici di condotta approvati

Fatti salvi i compiti e i poteri dell'Autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'Autorità di controllo competente.

Articolo 42. Certificazione

Gli Stati membri, le Autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente Regolamento dei trattamenti effettuati dai Titolari del trattamento e dai Responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese. La certificazione non riduce la responsabilità del titolare del trattamento o del responsabile riguardo la conformità al presente regolamento e lascia impregiudicati i compiti ed i poteri delle autorità di controllo competenti.

Articolo 43. Organismi di certificazione

Il Regolamento prevede il coinvolgimento di Organismi di certificazione accreditati per valutare la conformità dei sistemi di protezione dei dati attivati dai Titolari o dai Responsabili del trattamento soggetti al Regolamento.

Articolo 44. Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il Titolare del trattamento e il Responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente Regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente Regolamento non sia pregiudicato.

Articolo 45. Trasferimento sulla base di una decisione di adeguatezza

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato.

Articolo 46. Trasferimento soggetto a garanzie adeguate

In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il Titolare del trattamento o il Responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Articolo 47. Norme vincolanti d'impresa

Nel 2010 la Commissione europea ha adottato una nuova serie di clausole contrattuali tipo per i trasferimenti di dati tra Responsabili e incaricati del trattamento in risposta all'ampliamento delle attività di trattamento e, in particolare, all'emergere di nuovi modelli aziendali per il trattamento internazionale dei dati personali. Le clausole contrattuali tipo del 2010 contengono specifiche disposizioni che consentono, a determinate condizioni, di affidare le attività di trattamento a sub incaricati, offrendo al contempo sufficienti garanzie riguardo ai dati personali trasferiti.

Articolo 48. Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Le sentenze di un'Autorità giurisdizionale e le decisioni di un'Autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un Titolare del trattamento o di un Responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

Articolo 49. Derghe in specifiche situazioni

Il legislatore comunitario ha previsto delle deroghe ai principi da esso stesso stabiliti per autorizzare il trasferimento di dati personali verso Paesi extra UE presso i quali le condizioni in cui avviene il trattamento dei dati personali non sono conformi alle prescrizioni comunitarie.

Articolo 50. Cooperazione internazionale per la protezione dei dati personali

Il Garante italiano, già nella Relazione annuale 1997 (relativa al suo primo anno di attività) rimarcò la importanza di un rapporto cooperativo con altri organismi internazionali, anche prestandosi assistenza reciproca, a partire da quelli di matrice comunitaria.

Articolo 51. Autorità di controllo

Ogni Stato membro dispone che una o più Autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«Autorità di controllo»)

Articolo 52. Indipendenza

Ogni Autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente Regolamento.

Articolo 53. Condizioni generali per i membri dell'Autorità di controllo

Gli Stati membri dispongono che ciascun membro delle rispettive Autorità di controllo sia nominato attraverso una procedura trasparente: -dal rispettivo parlamento; -dal rispettivo governo; -dal rispettivo capo di Stato; oppure -da un organismo indipendente incaricato della nomina a norma del diritto dello Stato membro.

Articolo 54. Norme sull'istituzione dell'Autorità di controllo

Ogni Stato dell'Unione ha la sua Autorità di controllo che è competente per la gestione dei reclami a essa proposti o di eventuali violazioni del regolamento europeo e delle norme nazionali in materia di protezione dei dati, se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro. Ha il potere di irrogare sanzioni, conoscere direttamente delle controversie in materia di dati personali, e di effettuare controlli preventivi e chiedere comunicazioni nel caso di trattamenti particolarmente delicati.

Articolo 55. Competenza

Ogni Autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente Regolamento nel territorio del rispettivo Stato membro.

Articolo 56. Competenza dell'Autorità di controllo capofila

L'Autorità di controllo, individuata in relazione allo stabilimento principale o nel caso di stabilimento unico del Titolare o del Responsabile, agisce in qualità di Autorità di controllo capofila, per quanto attiene ai trattamenti transfrontalieri effettuati dal suddetto Titolare o Responsabile.

Articolo 57. Compiti

I compiti in capo all'Autorità di controllo sono, in buona sostanza, quelli già previsti dalla precedente normativa di settore.

Articolo 58. Poteri

Ogni Autorità di controllo ha tutti i poteri di indagine seguenti: a) ingiungere al Titolare del trattamento e al Responsabile del trattamento e, ove applicabile, al rappresentante del Titolare del trattamento o del Responsabile del trattamento, di fornirle ogni informazione di cui necessita per l'esecuzione dei suoi compiti; b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati; c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7; d) notificare al Titolare del trattamento o al Responsabile del trattamento le presunte violazioni del presente Regolamento; e) ottenere, dal Titolare del trattamento o dal Responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e f) ottenere accesso a tutti i locali del Titolare del trattamento e del Responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

Articolo 59. Relazioni di attività

Ogni Autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco delle tipologie di violazioni notificate e di misure adottate a norma dell'articolo 58, paragrafo 2.

Tali relazioni sono trasmesse al parlamento nazionale, al governo e alle altre Autorità designate dal diritto dello Stato membro. Esse sono messe a disposizione del pubblico, della Commissione e del comitato.

Articolo 60. Cooperazione tra l'Autorità di controllo capofila e le altre Autorità di controllo interessate

L'Autorità di controllo capofila coopera con le altre Autorità di controllo interessate conformemente al presente articolo nell'impegno per raggiungere un consenso. L'Autorità di controllo capofila e le Autorità di controllo interessate si scambiano tutte le informazioni utili.

Articolo 61. Assistenza reciproca

Le Autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine d'attuare e applicare il presente Regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro.

Articolo 62. Operazioni congiunte delle Autorità di controllo

Se del caso, le Autorità di controllo conducono operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di Autorità di controllo di altri Stati membri.

Articolo 63. Meccanismo di coerenza

Il nuovo "meccanismo di coerenza" consente alle imprese con stabilimenti presenti in più Stati membri, oppure i cui trattamenti hanno per oggetto soggetti appartenenti a più Stati membri, di potere interloquire con un'unica Autorità garante per la protezione dei dati personali, quella dello Stato ove si trova la sede legale della impresa.

Articolo 64. Parere del comitato europeo per la protezione dei dati

Attraverso il Comitato europeo della protezione dei dati si mira a garantire l'uniformità (coerenza), per cui sarà attribuita, la competenza ad assumere ogni tipo di misura, nonché a esercitare eventuali poteri correttivi, all'Autorità del paese dove ha sede lo «stabilimento principale» della società.

Articolo 65. Composizione delle controversie da parte del comitato

È previsto un sistema di composizione delle controversie che si attiva nei seguenti casi:

- a) quando viene sollevata una obiezione a una decisione adottata dall'autorità capofila, la decisione vincolante si applica a tutte le questioni oggetto dell'obiezione pertinente e motivata.
- b) nel caso in cui sorga un contrasto sulla competenza delle autorità di controllo;
- c) nel caso di omessa richiesta di un parere da parte di una autorità di controllo nelle ipotesi di cui "all'articolo 64, paragrafo 1, o non si conforma al parere del comitato emesso a norma dell'articolo 64". (par. 1)

Articolo 66. Procedura d'urgenza

Qualora una autorità di controllo ravvisi una omissione a carico di un'altra autorità di controllo può chiedere, al comitato, un parere di urgenza o una decisione vincolante di urgenza. Il comitato deve esprimersi in merito al parere vincolante così come riguardo alla decisione di urgenza entro due settimane.

Articolo 67. Scambio di informazioni

La Commissione può adottare atti di esecuzione di portata generale per specificare le modalità per lo scambio di informazioni per via elettronica tra Autorità di controllo e tra le Autorità di controllo e il comitato, in particolare il modulo standard di cui all'articolo 64.

Articolo 68. Comitato europeo per la protezione dei dati

Il Comitato dei ministri del Consiglio d'Europa ha approvato nel corso degli anni successivi al 1981 numerose "Raccomandazioni" che affrontano vari settori connessi alla protezione dei dati personali. Tali raccomandazioni hanno rappresentato e rappresentano tuttora un punto di riferimento importante, in quanto fissano principi che sono stati ripresi e sviluppati in numerosi documenti (anche comunitari).

Articolo 69. Indipendenza

Viene sancita l'indipendenza del Comitato che per le sue specifiche funzioni non può subire interferenze da nessuno, ad eccezione del verificarsi delle ipotesi di cui all'art. 70, precisamente svolge attività di consulenza nei confronti della Commissione, su qualunque tematica attinente alla protezione dei dati personali; se quest'ultima fissa un termine per la risposta il Comitato deve attenersi (art. 70, paragrafo 2)

Articolo 70. Compiti del comitato

I compiti del comitato europeo per la protezione dei dati, sono descritti sulla base dell'articolo 30, paragrafo 1, della direttiva 95/46/CE, e prevedono ulteriori elementi, a motivo del più vasto ambito di attività del comitato all'interno dell'Unione e al di fuori. Per essere in grado di reagire a situazioni di emergenza, la Commissione può chiedere un parere fissando un termine entro il quale il comitato deve rispondere.

Articolo 71. Relazioni

L'articolo 71 obbliga il comitato europeo per la protezione dei dati a riferire annualmente sullo stato relativo alla protezione dei dati personali, sia all'interno che al di fuori della UE.
La relazione che viene stilata deve contenere anche un esame del grado di applicazione delle linee guida, delle raccomandazioni e delle migliori prassi.
La relazione non è fine a se stessa ma va pubblicata e trasmessa sia al Parlamento europeo che al Consiglio ed alla Commissione.

Articolo 72. Procedura

Mentre per le decisioni adottate dal comitato, il quorum richiesto è la maggioranza semplice, il funzionamento di questo organismo è demandato ad un regolamento interno che deve essere approvato da una maggioranza pari ai due terzi dei suoi membri.

Articolo 73. Presidente

Il comitato elegge un presidente e due vicepresidenti tra i suoi membri a maggioranza semplice. Il presidente e i vicepresidenti hanno un mandato di cinque anni, rinnovabile una volta.

Articolo 74. Compiti del presidente

Il presidente ha il compito di: a) convocare le riunioni del comitato e stabilirne l'ordine del giorno; b) notificare le decisioni adottate dal comitato a norma dell'articolo 65 all'Autorità di controllo capofila e alle Autorità di controllo interessate; c) assicurare l'esecuzione tempestiva dei compiti del comitato, in particolare in relazione al meccanismo di coerenza di cui all'articolo 63. 2. Il comitato europeo stabilisce nel proprio Regolamento interno la ripartizione dei compiti tra presidente e vicepresidenti.

Articolo 75. Segreteria

Il comitato dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati.

Articolo 76. Riservatezza

Se il comitato europeo lo ritiene necessario, le sue deliberazioni hanno carattere riservato, come previsto dal suo Regolamento interno.

Articolo 77. Diritto di proporre reclamo all'Autorità di controllo

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente Regolamento ha il diritto di proporre reclamo a un'Autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione. L'Autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Articolo 78. Diritto a un ricorso giurisdizionale effettivo nei confronti dell'Autorità di controllo

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'Autorità di controllo che la riguarda.

Articolo 79. Diritto a un ricorso giurisdizionale effettivo nei confronti del Titolare del trattamento o del Responsabile del trattamento.

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'Autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente Regolamento siano stati violati a seguito di un trattamento.

Articolo 80. Rappresentanza degli interessati

Nell'ottica di rafforzare la sicurezza dei dati, il Regolamento attribuisce alle Autorità nazionali indipendenti di protezione dei dati poteri di controllo e sanzionatori più incisivi (artt. 77-84). Tali Autorità potranno invero comminare, alle imprese che violano il Regolamento, sanzioni pecuniarie corrispondenti ad importi fissi oppure commisurate al volume d'affari delle imprese coinvolte nella violazione del Regolamento.

Articolo 81. Sospensione delle azioni

L'articolo prende in esame l'ipotesi in cui se l'Autorità giurisdizionale di uno Stato membro abbia conoscenza che lo stesso trattamento pende davanti un'Autorità di un altro Stato membro, può sospendere le azioni, dopo averne avuto conferma ufficiale dall'altra Autorità.

Articolo 82. Diritto al risarcimento e responsabilità

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal Titolare del trattamento o dal Responsabile del trattamento.

Articolo 83. Condizioni generali per infliggere sanzioni amministrative pecuniarie

Ogni Autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente Regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

Articolo 84. Sanzioni

Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente Regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

Articolo 85. Trattamento e libertà d'espressione e di informazione

Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente Regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria.

Articolo 86. Trattamento e accesso del pubblico ai documenti ufficiali

I dati personali contenuti in documenti ufficiali in possesso di un'Autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale Autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'Autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente Regolamento.

Articolo 87. Trattamento del numero di identificazione nazionale

Gli Stati membri possono precisare ulteriormente le condizioni specifiche per il trattamento di un numero di identificazione nazionale o di qualsiasi altro mezzo d'identificazione d'uso generale. In tal caso, il numero di identificazione nazionale o qualsiasi altro mezzo d'identificazione d'uso generale sono utilizzati soltanto in presenza di garanzie adeguate per i diritti e le libertà dell'interessato conformemente al presente Regolamento.

Articolo 88. Trattamento dei dati nell'ambito dei rapporti di lavoro

L'articolo 88 dispone che gli Stati membri hanno facoltà di adottare norme specifiche per il trattamento dei dati personali nei rapporti di lavoro, soprattutto allorché il trattamento avvenga per finalità di assunzione, esecuzione del contratto di lavoro, di gestione e pianificazione del lavoro, pari opportunità, salute e sicurezza e, per finire, protezione del patrimonio aziendale o del cliente.

Articolo 89. Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

L'articolo 89 stabilisce condizioni specifiche per il trattamento di dati personali per finalità storiche, statistiche e di ricerca scientifica, che deve avvenire nel rispetto della salvaguardia dei diritti e delle libertà dell'interessato. Ciò comporta l'adozione di misure organizzative al fine di trattare i dati personali solo se strettamente necessario (cd principio di indispensabilità), ragion per cui se le finalità sottese a suddetto trattamento sono comunque raggiunte si può procedere anche alla pseudonimizzazione.

Articolo 90. Obblighi di segretezza

L'articolo 90 autorizza gli Stati membri ad adottare norme specifiche per regolare l'accesso delle Autorità di controllo ai dati personali e agli edifici, se i responsabili del trattamento sono tenuti all'obbligo di segretezza.

Articolo 91. Norme di protezione dei dati vigenti presso chiese e associazioni religiose

Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell'entrata in vigore del presente Regolamento, corpus completi di norme a tutela delle persone fisiche con riguardo al trattamento, tali corpus possono continuare ad applicarsi purché siano resi conformi al presente Regolamento.

Articolo 92. Esercizio della delega

L'articolo 92 contiene le disposizioni standard per l'esercizio delle deleghe. Ciò consente al legislatore di delegare alla Commissione il potere di adottare atti non legislativi di portata generale che integrano o modificano determinati elementi non essenziali di un atto legislativo (atti quasi legislativi).

Articolo 93. Procedura di comitato

L'articolo 93 dispone la procedura di comitato necessaria per il conferimento delle competenze di esecuzione alla Commissione, nei casi in cui sono necessarie condizioni uniformi di esecuzione degli atti giuridicamente vincolanti dell'Unione.

Articolo 94. Abrogazione della direttiva 95/46/CE

La direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018.

Attraverso il presente Regolamento è stata, quindi, disposta l'abrogazione della Direttiva 95/46/CE, che è la "direttiva madre" in materia di protezione dei dati personali che, però, a distanza di due decenni, ha finito con il mostrare tutti i limiti legati ad una materia rispetto alla quale la tecnologia ha rivoluzionato sia gli strumenti legati al trattamento dei dati personali sia i nuovi scenari che si sono delineati.

Articolo 95. Rapporto con la direttiva 2002/58/CE

Il presente Regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.

Articolo 96. Rapporto con accordi precedentemente conclusi

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che comportano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima di 24 maggio 2016 e conformi al diritto dell'Unione applicabile prima di tale data.

Articolo 97. Relazioni della Commissione

Entro 25 maggio 2020 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio relazioni di valutazione e sul riesame del presente Regolamento.

Articolo 98. Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati

Se del caso, la Commissione presenta proposte legislative di modifica di altri atti legislativi dell'Unione in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento. Ciò riguarda in particolare le norme relative alla protezione delle persone fisiche con riguardo al trattamento da parte di istituzioni, organi, uffici e agenzie dell'Unione e le norme sulla libera circolazione di tali dati.

Articolo 99. Entrata in vigore e applicazione

Il presente Regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea. Esso si applica a decorrere da 25 maggio 2018. Il presente Regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Informativa

Il regolamento conferma che ogni trattamento deve avere il proprio fondamento in una idonea base giuridica.

I fondamenti di liceità, previsti dall'art. 6 del GDPR, coincidono grossomodo con quelli previsti dal Codice: consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi a cui i dati vengono comunicati.

L'art. 13 del GDPR elenca in modo puntuale quanto il titolare deve sempre indicare in un'informativa:

- I contatti del DPO (se nominato)
- La base giuridica del trattamento
- Se sussiste la possibilità di trasferimento dei dati personali in Paesi terzi o ad organizzazioni internazionali
- Il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo
- Il diritto di presentare un reclamo all'autorità di controllo
- Se il trattamento comporta processi decisionali automatizzati o comportamenti profilazione
- Se i dati non sono raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine non superiore ad un mese dalla raccolta, oppure al momento della registrazione dei dati e/o dell'utilizzo degli stessi.

Il regolamento specifica quali debbano essere le caratteristiche dell'informativa:

Deve avere forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile.

Deve essere scritta in un linguaggio chiaro e semplice.

Viene consegnata in forma prevalentemente scritta e in formato elettronico (sono comunque ammessi altri mezzi)

Per quanto riguarda l'esonero dall'informativa, il Regolamento sottolinea che spetta al Titolare del Trattamento valutare se questa rappresenti uno sforzo sproporzionato.

Il consenso dell'interessato al trattamento dei dati personali dovrà essere, come oggi, preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita casella in un sito web). Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito». Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento. I trattamenti effettuati fino a quel momento dal titolare sulla base del consenso rimarranno comunque legittimi

Tempi dell'informativa:

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato – art. 13 del regolamento).

Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati.

Ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Consenso

Per i dati "sensibili" deve essere esplicito e lo stesso vale rispetto a decisioni basate su trattamenti automatizzati;

Non deve essere per forza documentato per iscritto, né è richiesta la forma scritta (anche se questa rimane la modalità più adeguata per provare in maniera inequivoca e l'esistenza di un consenso esplicito).

Il Titolare del trattamento deve essere in grado di dimostrare che l'interessato lo ha prestato per uno o più trattamenti specifici.

Per i minori è valido a partire dai 16 anni, prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

Il consenso deve essere sempre libero, specifico, informato e inequivocabile (non è ammesso infatti il consenso tacito o presunto) e deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

LA PRESENTE AZIENDA NON RACCOGLIE NE' GESTISCE DATI DI MINORI