Misure attuative del Regolamento 2016/679

del Parlamento Europeo e del Consiglio del 27 aprile 2016

Questionario di autovalutazione

sulla conformità al Regolamento UE 679/2019

sulla protezione dei dati personali

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Dipartimento \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | | | |
| Semestre \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Anno \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
|  | Quesiti | Valutazione | | | Precisazioni e approfondimenti |
|  |  | Raggiunto | Parzialmente raggiunto | Non raggiunto |  |
| 1 | I trattamenti di categorie particolari di dati, che possono rivelare l’origine razziale ed etnica, convinzioni religiose, filosofiche, ecc., opinioni politiche, adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, stato di salute e vita sessuale, vengono effettuati garantendo un elevato grado di sicurezza per i diritti e le libertà personali? |  |  |  |  |
| 2 | Le informative sono state integrate con le informazioni di cui all'art.13 e 14 Regolamento UE 679/2016? (Le informative devono contenere ulteriori informazioni rispetto a quelle contemplate nel D.Lgs.196/2003 ad es. tempo di conservazione dei dati, base giuridica del trattamento, legittimo interesse del titolare, etc.). |  |  |  |  |
| 3 | Per i trattamenti che vengono effettuati sulla base del consenso rilasciato dagli interessati qual’è il grado di aderenza all’art. 7 del Regolamento? Ai sensi dell’art 7 del Regolamento, se il consenso dell’interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L’interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. Il consenso è revocato con la stessa facilità con cui è accordato. Il titolare deve essere in grado di dimostrare che l’interessato ha prestato il proprio consenso |  |  |  |  |
| 4 | Viene aggiornato periodicamente il registro delle attività di trattamento del Titolare? Art.30 c.1 Regolamento. (Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità) |  |  |  |  |
| 5 | Viene aggiornato periodicamente il registro delle categorie di trattamento di trattamento del Responsabile? Art.30 c.2 Regolamento (Ogni responsabile del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità) |  |  |  |  |
| 6 | I Responsabili sono stati designati con atto esplicito da parte del Titolare? Art. 28 Regolamento Il Titolare designa un Responsabile del trattamento con un atto esplicito, quale un contratto o di altro atto giuridico equivalente, con il quale gli attribuisce specifici compiti ai sensi del Regolamento e nel quale vengono disciplinati la natura, durata e finalità dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal Titolare e, in via generale, delle disposizioni contenute nel Regolamento. |  |  |  |  |
| 7 | I soggetti che sono autorizzati al trattamento sono istruiti in tal senso dal Responsabile? Art.32 Comma 4 Regolamento Il titolare dei dati deve aumentare la sensibilizzazione e fornire la formazione a tutti i soggetti coinvolti nel trattamento dei dati personali. |  |  |  |  |
| 8 | I dipendenti hanno partecipato effettivamente a corsi o incontri sulla protezione dei dati personali? |  |  |  |  |
| 9 | E’ stata definita una procedura interna di gestione dei reclami degli interessati che definisca un iter operativo compatibile con i tempi massimi per il riscontro? |  |  |  |  |
| 10 | Sono state messe in atto misure tecniche per assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? Art.32 Regolamento |  |  |  |  |
| 11 | Le procedure relative al backup dei dati, al ripristino e ai test di ripristino sono adeguatamente documentate? Art.32 Regolamento |  |  |  |  |
| 12 | Esistono procedure per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento? Art.32 Regolamento |  |  |  |  |
| 13 | Si sta predisponendo la procedura per la realizzazione della valutazione di impatto? (PIA) Art.35 Regolamento 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. |  |  |  |  |
| 14 | Si sono verificate violazioni di dati personali nel semestre? (Data Breach) |  |  |  |  |
| 15 | Sono state notificate violazioni di dati personali al Garante per la protezione dei dati personali? Art.33 Regolamento 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 |  |  |  |  |
| 16 | Nelle questioni riguardanti la protezione dei dati personali ed in particolare nei processi di definizione di nuovi trattamenti per contribuire alla protezione dei dati sin dalla fase di progettazione e per impostazione predefinita è stato coinvolto il Responsabile protezione dei dati? |  |  |  |  |
|  | Il Referente Privacy  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Il Dirigente Generale  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |