DIRITTO24

L'ampliamento della definizione di dato personale

LINK: http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2018-05-16/l-ampliamento-definizione-dato-personale-155310.php

L'ampliamento della definizione di dato personale Avv. Eleonora Caravà - Studio Legale R&P Legal, Associate | 17/05/2018 07:19 Tweet My24 Aumenta dimensione font Diminuisci dimensione font Stampa l'articolo Invia articolo per email Privacy e cyber security, la nuova sezione de "I Consigli della Redazione " di PlusPlus 24 Diritto, costituita dalle ricerche realizzate in vista dell'imminente entrata in vigore del GDPR (Regolamento UE 679/2016 - entrata in vigore 25 maggio 2018) ed al prossimo termine per il recepimento della Direttiva NIS (Direttiva UE 1148/2016 - termine 09 maggio 2018) . Consultazione riservata agli abbonati di Plusplus24 Diritto - clicca qui *** Scheda sintetica tratta da "Privacy, la nuova disciplina europea" Avv. Eleonora Caravà - Studio Legale R&P Legal, Associate Scheda privacy Introduzione al GPDR Scheda privacy La nuova disciplina europea: novità nel settore bancario *** DEFINIZIONE DI DATO PERSONALE L'articolo 4, paragrafo 1, n. 1, del Gdpr definisce il Dato personale come "qualsiasi informazione riguardante una persona fisica identificata o identificabile". Per stabilire l'identificabilità di un Interessato, il Gdpr suggerisce di considerare tutti i mezzi (come l'individuazione) di cui il Titolare o un terzo può ragionevolmente avvalersi per identificare detto Interessato, direttamente o indirettamente. Gli Interessati possono essere associati ad identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati (quali gli indirizzi IP) a marcatori temporanei (cookies) o a identificativi di altro tipo (come i tag di identificazione a radiofrequenza) che possono lasciare tracce che, se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili e per identificare gli Interessati (si veda considerando 30 del Gdpr). NUOVE CATEGORIE DI DATI Il Gdpr ha introdotto nelle definizioni nuove categorie di Dati, tra cui quelli genetici e biometrici. Ha inoltre espressamente definito i dati relativi alla salute (i "Dati sanitari"). L'articolo 4, paragrafo 1, n. 13, del Gdpr definisce i dati genetici come quei Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di un Interessato che forniscono informazioni univoche sulla sua fisiologia o salute e che risultano dall'analisi di un suo campione biologico (i "Dati genetici"). L'articolo 4, paragrafo 1, n. 14, del Gdpr definisce i dati biometrici come quei Dati personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di un Interessato che ne consentono o confermano l'identificazione univoca, come l'immagine facciale o i dati dattiloscopici (i"Dati biometrici"). L'articolo 4, paragrafo 1, n. 15, del Gdpr definisce i Dati sanitari come quei Dati personali attinenti alla salute fisica o mentale di un Interessato, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute. CONSEGUENZE PRATICHE In caso di dubbi sull'interpretazione o identificazione di un'informazione come Dato personale, si suggerisce di trattare quell'informazione come se fosse un Dato personale, nella sua più ampia accezione. In considerazione del fatto che il Gdpr ha introdotto un sistema di compliance privacy più rigido, connotato - in caso di violazione delle disposizioni del Regolamento - da sanzioni pecuniarie particolarmente elevate, si suggerisce, al fine di minimizzare i rischi, di non trattare, quando è possibile, Dati personali, oppure, nel caso in cui vadano trattati, di adottare tutte le più opportune misure tecniche e organizzative (le "Misure di sicurezza") per conformarsi ai Gdpr. Se c'è un elevato grado di identificabilità dell'Interessato e i suoi Dati personali vanno

trattati, si suggerisce di usare la tecnica della pseudonimizzazione. SALVO L'ACCOUNTABILITY, IL GDPR NON MODIFICA IL "NOCCIOLO DURO" I PRINCIPI DELLA PRIVACY Sebbene i principi applicabili al Trattamento siano pressoché gli stessi della Direttiva madre, la vera novità è il principio di responsabilizzazione del Titolare (cosiddetto "accountability"). Titolari e/o Responsabili hanno un generale obbligo di implementare Misure di sicurezza appropriate al fine di comprovare il rispetto del Gdpr nello svolgimento dei Trattamenti. ACCOUNTABILITY Il Titolare del Trattamento deve esser sempre "pronto" a dimostrare di aver rispettato e di essersi conformato alle nuove disposizioni introdotte con il Gdpr. Attenzione: se il Titolare non può soddisfare i principi privacy del Gdpr e non sussistono esenzioni o deroghe in tal senso, il Trattamento da questo posto in essere è illecito, indipendentemente dalla natura giuridica dell'organizzazione del Titolare o dal settore in cui esso opera. Tra le nuove Misure di sicurezza che devono essere implementate dal Titolare vi sono: - il registro delle attività di Trattamento (il "Registro dei trattamenti" o il "Registro"); - la designazione del Data Protection Officer ("Dpo"), laddove obbligatoria o, se del caso, opportuna; - lo svolgimento delle Valutazione di Impatto Privacy ("Vip") o, usando la terminologia inglese, il Data Protection Impact Assessment ("Dpia"); - Privacy by Design / by Default; e - la notifica della violazione dei Dati personali ("Data breach"). Con il Gdpr "spariranno" le verifiche preliminari: il principio dell'accountability "scarica" sul Titolare tutta la responsabilità per i Trattamenti. CONSIGLI PRATICI Per prepararsi al Gdpr, i Titolari devono assicurarsi che i Trattamenti da loro effettuati siano conformi ai principi privacy previsti dall'articolo 5, paragrafo 1, del Regolamento, tra i quali particolare rilievo assumono quelli della trasparenza e della minimizzazione dei Dati. I Titolari - siano essi imprese o Pubblica amministrazione - devono rivedere ed aggiornare gli esistenti programmi di compliance privacy. I Titolari devono sviluppare o, laddove già esistenti, aggiornare le policy interne e i piani di risposta alle violazioni dei Data breach. In considerazione dell'armonizzazione introdotta dal Gdpr in tutto il territorio dell'Unione in tema di requisiti privacy, i gruppi multinazionali dovranno implementare policy interne e piani di risposta ai Data breach che abbiano una diffusione e applicazione quantomeno europea. Tra i vari fondi e risorse economiche accantonate dai Titolari e destinate alla compliance privacy, una buona parte dovrà esser dedicata alla formazione dei Dpo e del personale interno. I programmi di formazione dovranno esser strutturati in modo da offrire una conoscenza generale e complessiva del Gdpr, ma soprattutto dovranno adattare e "calare" la privacy nel settore in cui opera il Titolare. I Titolari dovranno assicurare che i Trattamenti effettuati e la conservazione dei Dati personali (intesi in senso ampio) siano limitati a quanto strettamente necessario. QUANDO UN TRATTAMENTO DI DATI PERSONALI È LECITO LA LICEITÀ DEL TRATTAMENTO Un Trattamento di Dati personali è lecito se e nella misura in cui è permesso ai sensi del Gdpr. Se il Titolare del Trattamento non agisce in virtù di una base giuridica legittima prevista dal Gdpr e non sussistono esenzioni o deroghe in tal senso, allora il Trattamento è prima facie illegittimo e si rischia di incorrere in severe sanzioni (amministrative e penali). Attenzione: tutti i tipi di imprese, indipendentemente dalla loro natura giuridica e dal settore in cui operano, e la Pubblica amministrazione sono tenute a trattare i Dati personali in modo lecito. Sotto questo punto di vista non esistono deroghe! Il Gdpr obbliga i Titolari ad individuare ed esporre nell'informativa privacy (l'"Informativa") le ragioni che giustificano il Trattamento dei Dati personali e gli scopi del Trattamento (le "Finalità"). Una novità rispetto alla Direttiva madre è l'articolo 11, paragrafo 1, del Gdpr che esenta il Titolare dal conservare, acquisire o trattare Dati personali ulteriori per identificare l'Interessato quando le Finalità del Trattamento non lo richiedono. Con l'articolo 6 del Gdpr, rimane pressoché immutato l'obbligo, già previsto dalla Direttiva madre, di trattare lecitamente i Dati personali. Le condizioni di legittimità che il Gdpr conferma rispetto all'impianto precedente sono: - il consenso, e cioè la volontà libera, specifica e informata manifestata dall'Interessato acché i suoi Dati personali siano fatti oggetto di Trattamento (il "Consenso"); - l'esecuzione di un contratto; - l'adempimento di un obbligo legale; - l'esecuzione di un compito di interesse pubblico; - il perseguimento di un interesse legittimo (questa condizione non si applica ai Trattamenti effettuati dalla Pa nell'adempimento e

svolgimento delle sue funzioni). CONSIGLI PRATICI SULL'OSSERVANZA DELLE CONDIZIONI DI LICEITÀ I Titolari sono tenuti a riesaminare i Trattamenti attuali e ad assicurarsi che per ogni Trattamento, anche futuro, esista una base giuridica che lo giustifichi e, in caso di assenza, appurare quale sia l'esenzione o la deroga. Si consiglia di documentare sempre quale sia la base giuridica del Trattamento e di illustrare brevemente le ragioni d tale scelta. Quando la base giuridica del Trattamento è il Consenso dell'Interessato, i Titolari sono tenuti a dimostrare di averlo acquisito in conformità al Gdpr o, in caso contrario, a revisionare gli attuali meccanismi preposti alla raccolta del Consenso. Se, invece, detta base è un interesse legittimo, i Titolari sono tenuti a documentare e a mantenere traccia di simile base giuridica nel Registro . ALCUNE OSSERVAZIONI SULLE CONDIZIONI DI LICEITÀ DEL TRATTAMENTO Ai sensi dell'articolo 6, paragrafo 1, del Gdpr, un Trattamento è lecito solo se l'Interessato ha prestato il suo Consenso o se sussiste un'altra base giuridica legittima prevista dal Gdpr. Sta, quindi, al Titolare dimostrare (e, questo, in un'ottica di accountability) che l'Interessato ha acconsentito al Trattamento dei suoi Dati personali (si veda considerando n. 42 e articolo 7, paragrafo 1. del Gdpr). Sebbene l'adempimento di un obbligo legale rimane, per il Titolare, una delle condizioni di liceità del Trattamento, il fatto che detto obbligo derivi dal diritto dell'Unione europea potrebbe mettere in difficoltà tutte quelle imprese - non stabilite nell'Unione - che possono essere destinatarie di un ordine giudiziario di esibizione di informazioni / Dati personali. L'articolo 6, paragrafo 1, lettera d), del Gdpr estende, rispetto alla Direttiva madre, la "salvaguardia degli interessi vitali" - di norma dell'Interessato - ad altre persone fisiche (ad esempio, i figli dell'Interessato). IL TRATTAMENTO DEI DATI SENSIBILI L'articolo 9 del Gdpr introduce dei cambiamenti in tema di Trattamento dei Dati sensibili. Il Trattamento lecito dei Dati sensibili presuppone un Consenso esplicito dell'Interessato. In ambito giuslavoristico, il Trattamento dei Dati sensibili è lecito se questo è necessario per consentire al datore di lavoro, quale Titolare, di adempiere gli obblighi previsti dal contratto di lavoro o quelli contemplati dalla sicurezza sociale o protezione sociale. In caso di incapacità, fisica o giuridica, dell'Interessato che non può prestare il proprio Consenso, e bisogna tutelare l'interesse vitale suo o di terzi, allora il Titolare può trattare i suoi Dati sensibili, sub specie di Dati sanitari. Non presente nella Direttiva madre, l'articolo 9, paragrafo 1, del Gdpr inserisce, tra i motivi che giustificano il Trattamento dei Dati sensibili: - il perseguimento di motivi di interesse pubblico, rilevante sulla base del diritto dell'Unione o degli Stati membri (lettera g); - i motivi di interesse pubblico nel settore della sanità pubblica come, ad esempio, la garanzia della sicurezza di prodotti medicinali (lettera i); - il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (lettera j). Plus Plus 24 Diritto L'upgrade dell'avvocato