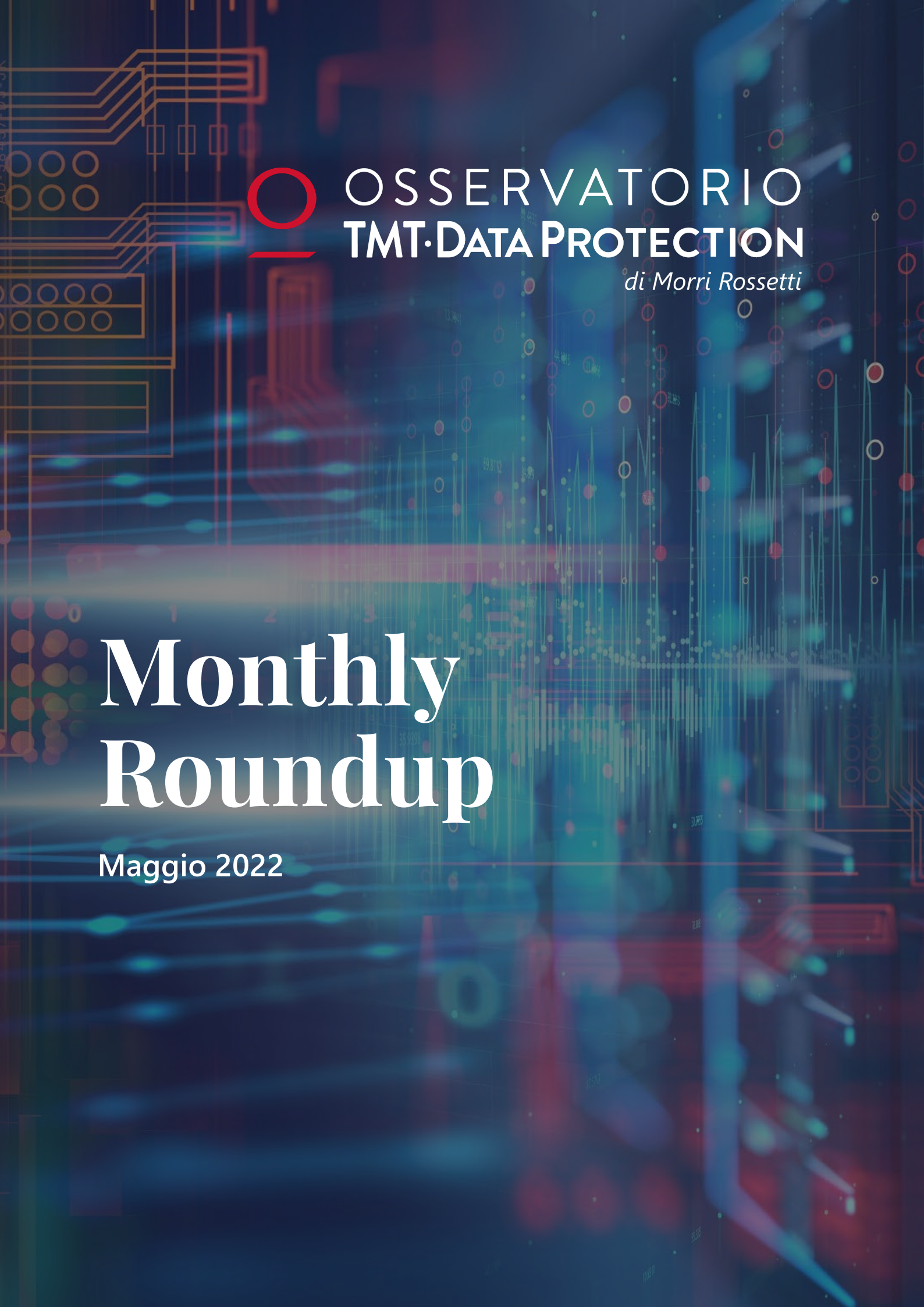

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Monthly Roundup

Maggio 2022

MONTHLY ROUNDUP

Maggio 2022

I principali aggiornamenti in materia di TMT & Data Protection del mese di Maggio 2022

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

- **EDPB**
  - Guidelines 04/2022 on the calculation of administrative fines under the GDPR [**Link**]
  - Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement [**Link**]
  - EDPB Annual Report 2021: Enhancing the depth and breadth of data protection [**Link**]

- **Garante Privacy**
  - Il Garante sanziona Uber per complessivi 4 milioni e 240mila euro [**Link**]
  - Email aziendale: il collaboratore esterno ha gli stessi diritti del dipendente [**Link**]
  - Telemarketing: sanzionata un'azienda per mancato riscontro a un cliente [**Link**]

PRINCIPALI AGGIORNAMENTI

Email aziendale: il collaboratore esterno ha gli stessi diritti del dipendente

Lo scorso 7 aprile 2022, l'Autorità Garante per la protezione dei dati personali (il "**Garante**" o l'"**Autorità**") ha pubblicato un'ordinanza ingiunzione nei confronti della Società Palumbo Superyacht Ancona s.r.l. (la "Società") con la quale ha imposto alla stessa una sanzione pari a Euro 50.000 per aver gestito l'account di posta aziendale di una collaboratrice esterna in violazione della normativa applicabile in materia di protezione dei dati personali.

Sul tema, trovano applicazione le *"Linee Guida del Garante per posta elettronica e internet"* ("**Linee Guida**") che, sebbene pubblicate nel 2007, sono tuttora applicabili in quanto compatibili con il Regolamento UE 679/2016 ("**GDPR**") e con il D.lgs. 196/2003, così come modificato dal D.lgs. 101/2018 ("**Codice Privacy**").

Si segnala inoltre che la tematica connessa alla gestione degli account di posta elettronica (sia in pendenza del rapporto lavorativo che a seguito della sua cessazione) è stata oggetto di numerosi provvedimenti dell'Autorità, attraverso i quali la stessa ha fornito importanti chiarimenti tra i quali,

ad esempio, le azioni da intraprendere per la dismissione e la conseguente cancellazione degli account di posta elettronica a seguito della cessazione del rapporto di lavoro, come meglio analizzate di seguito.

Premesso quanto sopra, il presente contributo ha lo scopo di chiarire, attraverso l'analisi della recente ordinanza ingiunzione del Garante emessa nei confronti della Società, se le azioni di dismissione e cancellazione degli account di posta elettronica aziendale indicate dal Garante per i lavoratori dipendenti, possano trovare applicazione anche con riferimento ai collaboratori esterni.

Descrizione del fatto

Nel settembre 2020, l'Autorità riceveva un reclamo da parte di una collaboratrice esterna della Società (l'"**Interessata**"), attraverso il quale la medesima rappresentava che la Società, senza alcun preavviso né comunicazione successiva, le aveva inibito l'accesso al suo account, utilizzato per le relazioni commerciali aziendali.

Tuttavia, nonostante quanto sopra rappresentato, l'account di posta assegnato all'Interessata risultava ancora attivo in quanto la stessa continuava a ricevere sul suo computer e sul telefono gli avvisi e le richieste di immettere la nuova password di accesso, nel frattempo cambiata dalla Società da remoto e a sua insaputa.

Considerato quanto sopra, l'Interessata aveva provveduto a segnalare l'accaduto alla Società, chiedendo il tempestivo ripristino della sua casella di posta aziendale, la quale conteneva comunicazioni sia di tipo lavorativo che personali.

Non avendo mai ricevuto risposta, l'Interessata si rivolgeva al Garante al fine di ricevere apposita tutala, considerando il comportamento della Società come lesivo del suo diritto alla riservatezza e del suo diritto costituzionalmente garantito alla segretezza della propria corrispondenza.

Conclusioni del Garante

A seguito dell'accertamento ispettivo, effettuato su mandato dell'Autorità dal Nucleo Speciale Privacy della Guardia di Finanza, e della chiusura dell'istruttoria, l'Autorità ha ribadito la presenza di obblighi informativi e di corretta e trasparente gestione della casella di posta aziendale a carico della Società, chiarendo altresì che:

- da un lato, il lavoratore deve essere sempre informato in maniera esaustiva sul trattamento dei suoi dati personali e il datore di lavoro deve rispettarne i diritti, le libertà fondamentali e la reputazione professionale.

Difatti, ai sensi delle Linee Guida, presupposto fondamentale affinché i controlli datoriali sulla casella di posta aziendale del dipendente in pendenza del rapporto di lavoro possano essere ritenuti legittimi è che la Società adempia agli obblighi informativi nei confronti del dipendente attraverso la pubblicazione di una policy interna e di un'apposita informativa, quest'ultima completa di tutti gli elementi di cui all'art. 13 del GDPR, volti a informare, preventivamente e in modo chiaro, i dipendenti circa le caratteristiche essenziali dei trattamenti che il datore di lavoro intende effettuare (ad esempio, finalità e modalità di conservazione e di accesso della società, individuazione delle specifiche e dettagliate attività di controllo), specificando in modo chiaro che l'account di posta elettronica aziendale deve essere utilizzato dai dipendenti solo ed esclusivamente per finalità aziendali e richiedendo di cancellare, laddove accidentalmente ricevute, eventuali mail personali non attinenti all'attività lavorativa.

Tali adempimenti, come ribadito dal Garante, servono a scongiurare l'aspettativa di riservatezza che i dipendenti (o i terzi) possano avere sulla

corrispondenza scambiata in costanza di rapporto di lavoro;

- dall'altro, la natura del rapporto di lavoro (i.e., lavoratore subordinato o collaboratore esterno) non rileva ai fini degli adempimenti privacy connessi alla corretta gestione dell'account aziendale assegnato al lavoratore o al collaboratore sia in pendenza di rapporto che a seguito della sua cessazione.

Con riferimento a quest'ultimo punto, giova ricordare che l'Autorità ha più volte chiarito[1] che le società che mantengono attivo l'account di posta aziendale di un dipendente dopo l'interruzione del rapporto di lavoro e accedono alle mail ivi contenute, pongono in essere un trattamento illecito di dati personali. Tuttavia, al fine di contemperare l'interesse delle società ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza sulla corrispondenza da parte degli ex dipendenti, l'Autorità ha indicato ai datori di lavoro una serie di misure tecnologiche da porre in essere, a seguito dello scioglimento del rapporto di lavoro, per non incorrere nell'ipotesi di cui sopra.

Nello specifico, le società devono:

i. disattivare l'*account* di posta elettronica dell'ex dipendente;
ii. contestualmente alla disattivazione, adottare sistemi automatici volti a informarne i terzi e a fornire a questi ultimi indirizzi alternativi ai quali inviare la corrispondenza collegata alle attività lavorative svolte dall'ex dipendente;
iii. adottare misure idonee a impedire alla stessa azienda la visualizzazione dei messaggi in arrivo durante il periodo in cui il predetto sistema automatico è in funzione; infine
iv. rimuovere l'*account* di posta elettronica aziendale dell'ex dipendente in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure di cui sopra.

Alla luce di quanto sopra, il Garante, oltre a comminare una sanzione pari a Euro 50.000, ha ordinato alla Società di consentire all'Interessata di accedere alla propria casella di posta per recuperare la sua corrispondenza e disattivare l'account informando clienti e fornitori con indirizzi alternativi.

Inoltre, il Garante ha chiarito che la Società non potrà trattare i dati estratti dalla casella di posta, se non per la tutela dei diritti in sede giudiziaria e solo per il tempo necessario a tale scopo, e dovrà altresì garantire un tempestivo riscontro all'esercizio dei diritti di tutti i suoi lavoratori, rilasciando loro un'idonea, preventiva e documentata informativa sul trattamento dei dati personali, incluso l'utilizzo di Internet e della posta elettronica aziendale.

* * *

SEGUE →

1 Ex multis, Provvedimento del Garante, concernente la disattivazione dell'account di posta elettronica dell'ex-dipendente n. 216 del 4 dicembre 2019.

Le nuove Linee Guida dell'EDPB sul calcolo delle sanzioni amministrative

In data 12 maggio 2022, *l'European Data Protection Board* ("**EDPB**") ha adottato le Linee Guida 04/2022 sul calcolo delle sanzioni amministrative (le "**Linee Guida**") al fine, *inter alia*, di armonizzare la metodologia utilizzata dalle autorità di protezione dei dati dei diversi Stati membri e di fornire una base chiara e trasparente per la determinazione delle sanzioni da parte delle stesse autorità.

Le Linee Guida integrano le precedenti linee guida sull'applicazione e la determinazione delle sanzioni amministrative pecuniarie ai fini del Regolamento 2016/679 ("**GDPR**"), adottate dal WP il 3 ottobre 2017 (WP253), aventi a oggetto l'individuazione delle circostanze in cui l'imposizione di una sanzione è da considerarsi uno strumento appropriato e un'interpretazione dei criteri di cui all'articolo 83 del GDPR. Pertanto, i due testi sono applicabili contemporaneamente e devono essere considerati complementari.

Le Linee Guida saranno sottoposte a consultazione pubblica per un periodo di 6 settimane. Dopo la consultazione pubblica, verrà adottata una versione finale delle stesse, tenendo conto dei feedback delle parti interessate, e includerà una tabella di riferimento con una serie di punti di partenza per il calcolo delle sanzioni, correlando la gravità di una violazione con il fatturato di un'impresa.

Calcolo dell'importo della sanzione e metodologia

Il calcolo dell'importo della sanzione è, infatti, a discrezione dell'autorità di controllo e deve avvenire nel rispetto delle norme previste dal GDPR. In particolare, il GDPR richiede che l'importo della sanzione sia effettivo, proporzionato e dissuasivo in ogni singolo caso (articolo 83, paragrafo 1, del GDPR). Inoltre, nel fissare l'importo della sanzione, le autorità di controllo devono tenere in debito conto un elenco di circostanze pertinenti la situazione specifica che si riferiscono alle caratteristiche della violazione (quali, la sua natura, gravità e durata; il carattere doloso o colposo; le categorie di dati personali interessate) o del carattere dell'autore (quali, il grado di responsabilità; eventuali precedenti violazioni commesse dallo stesso; il grado di cooperazione con l'autorità di controllo) (articolo 83, paragrafo 2, del GDPR). Infine, l'importo della sanzione non può superare i massimali previsti dall'articolo 83, paragrafi 4, 5 e 6, del GDPR – che in ragione delle violazioni commesse – sono individuati in un **importo fino a 10 milioni di euro** o, per le imprese, **fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore, o **fino a 20 milioni di euro** o, per le imprese**, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore.

La quantificazione dell'importo della sanzione si basa, quindi, su una valutazione specifica effettuata in ciascun caso, all'interno dei parametri previsti dal GDPR. Infatti, come altresì precisato nelle Linee Guida, sebbene l'obiettivo sia quello di creare punti di partenza armonizzati che consentano di sviluppare un orientamento comune, il contenuto delle Linee Guida non può essere specifico al punto di consentire a titolari/responsabili di effettuare un calcolo matematico dell'eventuale importo della sanzione, in quanto l'importo finale della

sanzione dipenderà sempre dalle circostanze del singolo casa concreto.

Le Linee Guida includono, quindi, i "punti di partenza" armonizzati per il calcolo di una sanzione. In particolare, vengono presi in considerazione tre elementi: la categorizzazione delle violazioni in base alla natura della violazione, la gravità della stessa e il fatturato di un'impresa.

Inoltre, alla luce di quanto previsto dal GDPR, l'EDPB ha sviluppato una metodologia di calcolo che si suddivide in 5 fasi:

1. in primo luogo, l'Autorità di controllo di volta in volta competente deve stabilire se il caso in questione riguarda uno o più casi di condotta sanzionabile e se questi hanno comportato a una o più violazioni. Nel dettaglio, occorre quindi identificare le operazioni di trattamento nel caso specifico valutando l'applicazione dell'articolo 83, paragrafo 3 del GDPR. Lo scopo è quello di chiarire se tutte le violazioni o solo alcune di esse possono essere sanzionate;

2. in secondo luogo, l'Autorità di controllo deve basarsi su un punto di partenza per il calcolo della sanzione per il quale l'EDPB fornisce un metodo armonizzato. In particolare, i punti di partenza vanno individuati sulla base di una valutazione:

• del tipo di violazione da ricondurre nelle ipotesi di cui all'articolo 83, paragrafi 4, 5 o 6 del GDPR;
• della gravità della violazione ai sensi dell'articolo 83, paragrafo 2, lettere a), b) e g) del GDPR;
• del fatturato dell'impresa quale uno degli elementi da tenere in considerazione al fine di imporre una sanzione che sia effettiva, proporzionata e dissuasiva, ai sensi dell'articolo 83, paragrafo 1 del GDPR

3. in terzo luogo, l'Autorità di controllo deve considerare i fattori aggravanti o attenuanti che possono aumentare o diminuire l'importo della sanzione (quali, le azioni intraprese dal titolare/responsabile per attenuare il danno subito dagli interessati; il grado di responsabilità; precedenti violazioni, etc.), per i quali l'EDPB fornisce un'interpretazione coerente con le precedenti linee guida del Working Party;

4. la quarta fase consiste nel determinare i massimali legali delle sanzioni, come stabilito dall'articolo 83, paragrafi 4, 5 o 6 del GDPR e garantire che tali importi non vengano superati;

5. nella quinta e ultima fase, l'autorità di controllo competente deve di volta in volta analizzare se l'importo finale calcolato soddisfi i requisiti di effettività, proporzionalità e dissuasività e o se siano necessari ulteriori adeguamenti dell'importo.

All'interno delle Linee Guida ad ogni fase sopra richiamata viene dedicato uno specifico capitolo volto a fornire maggiori chiarimenti in merito all'analisi da svolgere, fornendo altresì esempi pratici.

Nozione di impresa e determinazione del fatturato

Nell'ambito dell'analisi della fase 4 della metodologia sviluppata, il capitolo 6 delle Linee Guida ("*Legal maximum and corporate liability*") si sofferma anche sulla nozione di impresa e sulla determinazione del fatturato.

Il GDPR fornisce indicazioni in merito alla nozione di impresa ai fini della determinazione delle sanzioni. In particolare, il considerando 150 del GDPR afferma che "[...]. *Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli*

*101 e 102 del Trattato sul Funzionamento dell'Unione europea ("***TFUE***") a tali fini*".

Pertanto, l'articolo 83, paragrafi 4, 5 e 6 **si basa sul concetto di impresa di cui agli articoli 101 e 102 del TFUE**, fatti salvi l'articolo 4, paragrafo 18, del GDPR (che fornisce una definizione di impresa) e l'articolo 4, paragrafo 19, del GDPR (che definisce la definizione di gruppo di imprese). Il primo concetto di impresa viene per lo più utilizzato nel Capitolo V del GDPR nella frase gruppo di imprese impegnate in un'attività economica comune. Inoltre, il termine è applicato in senso generale, non come destinatario di una disposizione o di un obbligo.

Di conseguenza, nei casi in cui il titolare/responsabile sia (parte di) un'impresa ai sensi degli articoli 101 e 102 del TFUE, come indicato nelle Linee Guida, **il fatturato combinato di tale impresa nel suo complesso può essere utilizzato per determinare il limite massimo dinamico della sanzione** e per garantire che la sanzione derivante sia in linea con i principi di effettività, proporzionalità e dissuasività di cui al GDPR.

Sul punto, anche le precedenti linee guida del Working Party prevedevano *che "[a]l fine di irrogare sanzioni amministrative che siano effettive, proporzionate e dissuasive, l'autorità di controllo deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea ("***CGUE***") ai fini dell'applicazione degli articoli 101 e 102 TFUE, secondo cui il concetto di impresa va inteso come un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Conformemente al diritto e alla giurisprudenza dell'UE, un'impresa deve essere intesa quale unità economica che intraprende attività economiche/commerciali, a prescindere dalla persona giuridica implicata"*.

Dall'analisi delle sentenze della CGUE più rilevanti sul punto, emerge che la nozione di impresa ai sensi degli artt. 101 e 102 del TFUE, dev'essere intesa nel senso che essa si riferisce ad un'unità economica, anche qualora, sotto il profilo giuridico, tale unità economica sia costituita da più persone, fisiche o giuridiche. L'esistenza di un'unità economica può essere quindi dedotta da un complesso di elementi concordanti ancorché nessuno di tali elementi, isolatamente considerato, sia sufficiente per dimostrare l'esistenza di tale unità. Infatti, sebbene il concetto di impresa ai sensi del diritto europeo della concorrenza abbia una portata più ampia del concetto di impresa civilistico**, la sussistenza di "un'unità economica" deve essere comunque valutata in considerazione dei legami economici, giuridici e organizzativi tra le società del gruppo** che caratterizzano il caso di specie (quali, a titolo esemplificativo, l'ammontare della partecipazione, i legami personali o organizzativi, le istruzioni e l'esistenza di contratti infragruppo[2].

---

2 Il punto 124 delle Linee Guida prevede che nel caso specifico in cui una società madre detenga il 100% o quasi delle azioni di una società controllata che ha violato l'articolo 83 del GDPR e sia quindi in grado di esercitare un'influenza decisiva sul comportamento della sua società controllata, si presume che la società madre eserciti effettivamente tale influenza decisiva sul comportamento della sua società controllata (la cosiddetta presunzione Akzo). Ciò vale anche se la società madre non detiene direttamente le quote del capitale totale, ma indirettamente attraverso una o più società controllate. Ad esempio, potrebbe esserci una catena di società controllate, in cui un'entità detiene il 100% o quasi delle azioni di un'entità intermedia che detiene il 100% o quasi delle azioni di un'altra entità, e così via. Anche una società madre potrebbe detenere il 100% o quasi delle azioni di due entità che detengono ciascuna circa il 50% di un'entità, esercitando così un'influenza decisiva su tutte le entità. In tali circostanze, è sufficiente che l'autorità di vigilanza dimostri che la società controllata è direttamente o indirettamente posseduta interamente o quasi interamente dalla società

Quanto alla determinazione del fatturato, lo stesso deve essere ricavato dal bilancio annuale di un'impresa, redatto con riferimento all'esercizio commerciale e in grado di fornire una panoramica dell'esercizio passato di una società o di un gruppo di società (bilanci consolidati). Il fatturato è definito come la somma di tutti i beni e servizi venduti. Il termine fatturato ai sensi dell'articolo 83, paragrafi 4 e 5, del GDPR deve essere inteso in termini di fatturato netto ai sensi della direttiva 2013/34/UE60.

L'articolo 83, paragrafi 4-6, del GDPR stabilisce che deve essere utilizzato il fatturato mondiale totale annuo dell'esercizio finanziario precedente. Per quanto riguarda il tema di quale sia l'evento a cui si riferisce il termine "precedente", la giurisprudenza della CGUE in materia di diritto della concorrenza deve essere applicata anche per le sanzioni previste dal GDPR, in modo che **l'evento rilevante sia la decisione di irrogare la sanzione emessa dall'autorità di controllo e non il momento della violazione o la decisione del tribunale**. In caso di trattamento transfrontaliero, la decisione rilevante non è il progetto di decisione, ma piuttosto la decisione finale emessa dall'autorità di controllo capofila ai fini della determinazione della sanzione.

Conclusioni

Posto che le Linee Guida discusse nel presente contributo sono ancora soggette alla fase di consultazione pubblica che durerà 6 settimane (decorse dalla data della loro pubblicazione), le stesse sono utili al fine di fornire maggior chiarezza sia per le autorità di controllo nell'esercizio dei loro poteri sanzionatori sia per tutti gli operatori economici tenuti al rispetto della normativa in materia di protezione dati personali.

Infatti, il tema della determinazione delle sanzioni pecuniarie presenta, ad oggi, alcune zone grigie che lasciano spazio a dubbi interpretativi, *in primis* e *inter alia*, quanto all'individuazione dell'impresa da sanzionare, qualora tale impresa operi nell'ambito di un gruppo imprenditoriale, e quindi all'individuazione del fatturato in base al quale determinare l'importo della sanzione.

Sul punto è possibile, infatti, ricordare alcuni provvedimenti sanzionatori del Garante Privacy italiano emessi nei confronti di importanti operatori italiani nell'ambito delle telecomunicazioni e dell'energia. Ferma l'analisi di cui sopra – e tenuto conto che il testo delle recenti Linee Guida risulta in linea con il testo delle precedenti adottate dal Working Party nel 2017 e con la giurisprudenza consolidata della CGUE – in tali casi, il Garante Privacy ha concluso

---

madre per presumere - come regola di esperienza pratica - che la società madre eserciti un'influenza determinante.
Il punto 125 continua precisando che la presunzione di Akzo non è assoluta, ma può essere confutata da altre prove. Per confutare la presunzione, la/e società deve/devono fornire prove relative ai legami organizzativi, economici e giuridici tra la società controllata e la sua controllante che siano in grado di dimostrare che essa non costituisce una singola unità economica ("SUE") nonostante detenga il 100% o quasi delle azioni. Per accertare se una società controllata agisce in modo autonomo, occorre tenere conto di tutti i fattori rilevanti relativi ai legami che legano la società controllata alla società madre, che possono variare da caso a caso e non possono quindi essere elencati in modo esaustivo.
Inoltre, come indicato nel punto 126, se, invece, la società madre non detiene la totalità o la quasi totalità del capitale, l'autorità di vigilanza deve dimostrare ulteriori elementi per giustificare l'esistenza di una SUE. In tal caso, l'autorità di vigilanza deve dimostrare non solo che la società madre ha la capacità di esercitare un'influenza decisiva sulla controllata, ma anche che l'ha effettivamente esercitata, in modo da poter intervenire in qualsiasi momento nella libertà di scelta della controllata e determinarne il comportamento. La natura o il tipo di istruzione è irrilevante nel determinare l'influenza della società madre.

per la determinazione di sanzioni di importi più bassi in ragione proprio dell'individuazione della base di calcolo non nel fatturato del gruppo quanto nel fatturato della singola impresa.

In particolare, nel provvedimento emesso nei confronti di TIM S.p.A., il Garante ha mitigato il carico sanzionatorio nei confronti della società determinando l'importo della sanzione anche alla luce dei criteri di effettività, proporzionalità e dissuasività di cui al GDPR.

In ragione di ciò, ha chiarito che *"in una complessiva ottica di necessario bilanciamento fra diritti degli interessati e libertà di impresa e in via di prima applicazione delle sanzioni amministrative pecuniarie previste dal Regolamento, occorre valutare prudentemente i suindicati vari criteri, anche al fine di limitare l'impatto economico della sanzione sulle esigenze organizzative, funzionali ed occupazionali della Società. Pertanto si ritiene che* - in base al complesso degli elementi sopra indicati, a fronte della sanzione edittale massima (556.058.923,00 euro, pari al 4% del fatturato di TIM, ossia 13.901.473.076 euro, e non del più elevato fatturato del gruppo Telecom) - *debba applicarsi alla medesima Società la sanzione amministrativa del pagamento di una somma pari allo 0,2% del suindicato fatturato corrispondente a euro 27.802.946,00)".*

* * *

Data breach: Ospedale milanese ammonito dal Garante Privacy a seguito di una violazione dei dati personali

In data 24 marzo 2022, l'Autorità Garante per la protezione dei dati personali ("**Garante**" o "**Autorità**") ha emesso il provvedimento n. 100, con cui ha ammonito un istituto di ricerca facente parte del sistema sanitario nazionale (l'"**Istituto**") per aver violato le disposizioni di cui agli artt. 5, comma 1, lettere a) e f), 9 e 32 del Regolamento (UE) 2016/679 ("**GDPR**"), a seguito di una violazione dei dati personali dallo stesso subìta e prontamente notificata al Garante.

Descrizione del fatto

Nell'aprile del 2021, l'Istituto aveva notificato al Garante, ai sensi dell'art. 33 del GDPR, un data breach causato da un'azione accidentale interna e consistito nell'invio, tramite posta, di un plico contenente un referto radiologico e un CD al destinatario sbagliato

Tale violazione aveva dunque comportato la perdita di confidenzialità dei dati anagrafici e dei dati relativi alla salute di un paziente (i.e. referto e CD relativi alla risonanza magnetica).

Tuttavia, i rischi per le libertà e i diritti degli interessati connessi a suddetta violazione venivano stimati dall'Istituto come "bassi" in quanto:

- i dati personali coinvolti dalla violazione erano riferibili a un solo interessato;
- il paziente (che per errore aveva ricevuto la documentazione di un altro soggetto)

aveva tempestivamente provveduto a distruggere il referto e il CD.

Nonostante quanto sopra, l'Istituto, in ottemperanza di quanto disposto dall'art. 34 del GDPR, aveva notificato prontamente la violazione all'interessata i cui dati personali erano stati erroneamente comunicati a un terzo soggetto non autorizzato a riceverli e, contestualmente, al fine di prevenire simili violazioni future, aveva organizzato un "*re-training*" sulle le misure di sicurezza per tutto il personale amministrativo della radiologia.

Conclusioni del Garante

All'esito dell'attività istruttoria svolta dall'Autorità, quest'ultima aveva riscontrato un trattamento illecito di dati personali dovuto alla violazione, da parte dell'Istituto, dei seguenti principi:

- il principio di liceità del trattamento di cui all'art. 5, comma 1, lett. a) del GDPR, a causa della comunicazione dei dati personali (anche relativi allo stato di salute) a un terzo non autorizzato, in assenza di un'idonea base giuridica.

Sul punto, infatti, il Garante ha precisato che in base al richiamato principio, i dati di categoria particolare di cui all'art. 9 del GDPR possono essere trattati solo in presenza di una delle specifiche ipotesi di esenzione dal divieto di trattamento di tali dati, individuate al comma 2 del medesimo articolo (quali, a titolo esemplificativo e non esaustivo, il consenso dell'interessato, l'esistenza di specifici obblighi in materia di diritto del lavoro e della sicurezza sociale e della protezione sociale, la necessità di tutelare un interesse vitale dell'interessato, etc.).

Inoltre, l'Autorità ha specificato che, in ambito sanitario, la disciplina applicabile in materia di protezione dei dati personali prevede che le informazioni sullo stato di salute possano essere comunicate:

- al solo interessato; ovvero
- a terzi, ma unicamente sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso previa delega scritta di quest'ultimo[3];

- il principio di integrità e riservatezza dei dati personali di cui all'art. 5, comma 1, lett. f) e art. 32 del GDPR, a causa dell'assenza di adeguate misure tecniche e organizzative volte a prevenire simili violazioni di dati personali.

  A tal riguardo, l'Autorità ha chiarito che, al fine di garantire la sicurezza del trattamento, il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono (*inter alia*) la capacità di assicurare su base permanente la riservatezza dei dati e una procedura per testare, verificare e valutare regolarmente l'efficacia di tali misure.

In considerazione di quanto sopra esposto, il Garante ha qualificato la violazione in questione come "violazione minore" ai sensi del considerando 148 del GDPR[4], posto che:

3 Cfr. Art. 9 del GDPR e Art. 83 del Codice Privacy (i.e. D.lgs. 196/2003) in combinato disposto con l'art. 22, comma 11, D.Lgs. 10 agosto 2018, n. 101; cfr. anche provv. generale del 9 novembre 2005 - doc. web n. 1191411, ritenuto compatibile con il GDPR e con le disposizioni del decreto n. 101/2018; cfr. art. 22, comma 4, del citato D.Lgs. n. 101/2018.

4 Considerando 148 del GDPR: "Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento.

In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria.
Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a

- l'episodio risultava isolato e determinato da un'azione accidentale interna;
- la violazione era stata di breve durata e aveva coinvolto un unico interessato;
- il referto oggetto di errata comunicazione non conteneva la diagnosi clinica del paziente, ma esclusivamente il numero di classificazione radiologica e la radiografia stessa;
- l'Istituto si era prontamente attivato notificando l'evento all'Autorità, comunicando la violazione all'interessato e prevedendo l'implementazione di nuove e specifiche misure organizzative volte a prevenire il ripetersi di violazioni simili in futuro; e
- l'interessata non aveva subito danni dall'evento occorso.

Per tali ragioni, il Garante ha ritenuto sufficiente ammonire l'Istituto, richiedendo allo stesso di provvedere a rispettare le previsioni del GDPR e non anche sanzionare l'Istituto stesso, non ritenendo sussistenti i presupposti per l'adozione di ulteriori provvedimenti correttivi, atteso che erano state disposte misure organizzative volte ad evitare il ripetersi di episodi come quello segnalato.

* * *

EU and USA reach an 'agreement in principle' after the "Schrems II" decision

On the 25 of March 2022, the European Commission and the United States of America government have announced that an agreement in principle on a new Trans-Atlantic Data Privacy Framework ("**Framework**") has been reached.

The Framework, once adopted, will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union ("**CJEU**"), in the Schrems II decision of July 2020, which declared the invalidity of the "Privacy Shield" mechanism adopted for data flows between EU and US.

As also declared by the competent authorities, the commitment on the US side, on which has been based the agreement on principle for the adoption of the new Framework, is to implement reforms and adequate measures for the privacy and the protection of personal data of individuals in the European Economic Area ("EEA") when their data are transferred to the US.

Specifically, the new Framework reflects more than a year of negotiation between EU and US and takes into account the CJEU considerations and concerns raised in the Schrems II decision (namely, the US legislation did not meet the requirements of the EU law and did not grant data

un codice di condotta e eventuali altri fattori aggravanti o attenuanti.
L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo".

subjects enforceable legal rights against the US authorities).
In particular, the Framework shall ensure (as indicated in the Factsheet Trans-Atlantic Data Privacy Framework):

- data ability to flow freely and safely between the EU and participating US companies;
- a new set of rules and binding safeguards to limit access to data by US intelligence authorities to what is necessary and proportionate to protect national security;
- procedures to ensure effective oversight of new privacy and civil liberties standards that will be adopted by US intelligence agencies;
- a new two-tier redress system to investigate and resolve complaints of Europeans on access of data by US intelligence authorities, which includes a Data Protection Review Court;
- strong obligations for companies processing data transferred from the EU, including the requirement to self-certify their compliance to the principles through the US Department of Commerce;
- specific monitoring and review mechanisms.

On the 6 of April 2022, the European Data Protection Board ("**EDPB**") issued the Statement 01/2022 where welcomed the Framework. Notably, the EDPB recognises the commitment of the United States highest authorities to establish measures to protect the data of EEA-based individuals when transferred to the US.

However, it is worth noting that, since the Framework will now be translated into legal documents, the EDPB, in its Statement, declares that it "*will examine how this political agreement translates into concrete legal proposals to address the concerns raised by the Court of Justice of the European Union (CJEU) in order to provide legal certainty to EEA individuals and exporters of data*". Specifically, for issuing the adequacy decision for the Framework, the European Commission must follow a multi-step process: following a written proposal drafted by the European Commission, the EDPB will review and issue an opinion concerning such proposal.

In any case, the EDPB also specifies that the announcement of the European Commission and United States does **not constitute a legal framework on which data exporters can base their data transfers to the US**. Indeed, during any transfer, at this time, they must continue to comply with the principles outlined in the CJEU decision in Schrems II.

Reminder: How EU data exporters can transfer data to the United States?

In the context of the Schrems II decision, the CJEU reminded that the protection granted to personal data in EEA must travel with the data, notwithstanding where such data is transferred, and that the level of protection in third countries does not need to be identical to that guaranteed in the EU, but it must be essentially equivalent.

Subsequently, as recalled in the EDPB's FAQ adopted on the 23 of July 2020, in the absence of a decision pursuant to Article 45 of the Regulation (EU) 2016/679 ("**GDPR**") or of appropriate safeguards pursuant to Article 46 of the GDPR, according to Articles 46 and 49 of the GDPR, data exporters may transfer data to the US by adopting other mechanism.

Specifically, a transfer to a third country (or an international organisation) can only take place if EU data exporter has provided appropriate safeguards and if data subjects have enforceable rights and effective remedies (as provided in Article 46(1) and (2)(c) of the GDPR). The

appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by, among others, Standard Contractual Clauses ("**SCCs**") and Binding Corporate Rules ("**BCRs**").

The CJEU upheld the validity of the European Commission Decision 2010/87/EC on Standard Contractual Clauses, as a transfer tool that may serve to ensure contractually and essentially equivalent level of protection for data transferred to third countries, provided that the underlying transfers must be assessed on a case-by-case basis to determine whether the personal data will be adequately protected. On this regard, with reference to both the SCCs and the BCRs, the CJEU pointed out that:

- it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the relevant third country, in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice;
- if this is not the case, supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA should be adopted; the CJEU does not specify which measures these could be, it should be necessary to identify them on a case-by-case basis;
- in case the assessment determines that the data transferred pursuant to the SCCs or to the BCRs are not afforded a level of protection essentially equivalent to that guaranteed within the EEA, it will be necessary to immediately suspend the transfers or notify the competent supervisory authority.

On the 4 June of 2021, the European Commission published its final Implementing Decision adopting new standard contractual clauses for the transfer of personal data to third countries ("**New SCCs**"). New SCCs follow the draft decision published on the 12 of November 2020 and, among others, respond to the Schrems II decision. The New SCCs set out a process whereby the parties to the SCCs must undertake a transfer impact assessment and document the outcome, but provide no real guidance on what the outcome of that process should be.

On this regard, taking into consideration the necessity of carrying out a transfer risk assessment, the EDPB, with Recommendations 01/2020 "on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" published on the 10 of November 2020 and, then, adopted on the 18 of June 2021, has laid out a roadmap to help exporters in the phase of assessment of third countries level of protection and, where needed, in the identification of supplementary measures that must be put in place for certain data transfer.

The roadmap comprises the following six steps:

- know your transfer;
- verify the transfer tool your transfer relies on;
- assess the law of the third country;
- identify and adopt supplementary measures;
- take any formal procedural steps the adoption of your supplementary measure may require;
- periodically re-evaluate the security of transfers and monitor if there have been or there will be any developments that may affect it.

Moreover, according to Article 49 of the GDPR, it is still possible to transfer data from the EEA to the US only if at least one of the conditions set out in the par. 1 is met. Specifically, in the event that the transfers are:

- based on the data subjects' consent, such consent shall be explicit, specific for the particular data transfer or set of transfers and informed, particularly in relation to the possible risks of the transfer;
- necessary for the performance of a contract between the data subject and the controller, personal data may only be transferred when the transfer is objectively necessary for the performance of a contract and is occasional;
- necessary for important reasons of public interest (which must be recognized in EU or Member States' law), the essential requirement for the applicability of this derogation is that the public interest has to be important. It should be borne in mind that the importance of public interest does not mean that such data transfers can take place on a large scale and in a systematic manner: such derogations need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.

Furthermore, the EDPB on the 10 of November 2020 also adopted the Recommendations 02/2020 "on the European Essential Guarantees for surveillance measures" that provide elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be considered justifiable interference or not. On this regard, surveillance measures are considered justifiable with the following requirements:

- processing based on clear, precise and accessible rules;
- necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated;
- existence of an independent oversight mechanism should exist;
- availability to the individual of effective remedies.

In view of all of this, data exporters still have the chance to transfer data from the EEA to the US, but they must comply with the principles outlined in the CJEU decision in Schrems II and, in particular, with the above provisions, while waiting for the European Commission and the United States government to translate the new Framework into legal documents that will need to be adopted on both sides.

* * *

Per maggiori informazioni, potete contattare:

Carlo Impalà
Partner e Responsabile Dip. TMT e Data Protection
(Carlo.Impala@MorriRossetti.it)

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti

Morri Rossetti
Piazza Eleonora Duse, 2
20122 Milano

MorriRossetti.it
Osservatorio-dataprotection.it