normativo) è stato considerevolmente modificato, nel tentativo di generare una solida consapevolezza del valore dei dati personali e della loro protezione, accogliendo importanti principi (come, ad es. il principio di trasparenza, diritto all'oblio, principio di *accountability*, principio di *privacy by design*)[4].

L'approccio del Regolamento pone una vera e propria "rivoluzione": si passa da un modello di trattamento autorizzativo a un regime basato sulla *accountability*, vale a dire alla c.d. "responsabilizzazione"[5].

Peraltro, il Gdpr enuclea, specificatamente, due ambiti di applicazione[6]:

1) territoriale → la normativa si applica al trattamento 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*" (art 3, paragrafo 3, Reg. 679/2016); poi, ulteriormente chiarito considerando "*l'effettivo e reale svolgimento dei attività nel quadro di un organizzazione stabile*" (cfr. "Considerando", n. 22);

2) materiale → prevedendo, in questo senso, un sensibile ampliamento dell'ambito di applicazione e distinguendo:

a) "**dati identificativi**": che sono, tra l'altro, i c.d. "**dati personali**" (**nome, cognome, codice fiscale, numero di telefono, indirizzo residenza, email**) ed ivi includendo anche i c.d. "**dati biometrici**" (art. 4, co. 1, punto 13 e punto 14), ossia, ricavati da proprietà biologiche, aspetti comportamentali, caratteristiche fisiologiche, tratti biologici, etc. e, in particolari casi, anche gli indirizzi IP, i cookies, etc.);

b) "**dati particolari**": secondo l'art. 9 del Gdpr trattasi di "*dati personali che rivelino* ***l'origine raziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché 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*". Se ne deduce, quindi, che la normativa europea considera e pone protezione a tali "dati particolari" che, quindi, sono soggetti a trattamento speciale.

bb) Inoltre, anche i "**dati giudiziari**" (art. 10, Reg. 679/2016) sono inclusi in questa categoria tutti i dati riferiti ad aspetti relativi al casellario giudiziario ivi comprese pene inflitte e/o sentenze di condanna; anche essi, come tale, sottoposti a trattamento speciale.

---

[4] Ivi, 3.

[5] MESSINA CICCIA A., *La riforma della privacy. Guida pratica per l'applicazione del nuovo regolamento europeo (Gdpr)*, in *Italia Oggi*, serie speciale, num. 5, anno 28, 2018, spec. 12.

[6] MARTORANA M., TESORO A., BARBERISI A. (cur.), op. cit., 3.

Il legislatore europeo ha espressamente previsto che la categoria di dati c.d. "dati particolari" possono essere trattati solo nei casi espressamente previsti dall'art. 9, n. 2, Reg. 679/2016, vale a dire:

- quando l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

- quando il trattamento è necessario pe assolvere gli obblighi es esercitare i diritti specifici del "Titolare del trattamento" o dell'interessato in materia di diritto al 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;

- quando il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

- quando il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

- quando il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

- quando il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

- quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

- quando il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

- quando il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei

dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

- quando il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

- infine, quando i dati personali in questione sono trattati (per le finalità di cui al paragrafo 2, lettera h) del Reg. 679/2016), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

c) "**dati anonimi e pseudonimi**": sono tali i dati "anoniminizzati", ossia quei dati che sono stati privati di tutti gli elementi identificativi. A tal proposito, occorre ribadire che il Gdpr prevede che i dati siano conservati per un periodo di tempo limitato e, in particolare, non oltre il tempo necessario per raggiungere lo scopo alla base del trattamento. Invece, ben diversa è la circostanza che taluni dati dopo aver esaurito lo scopo del trattamento, siano comunque conservati per fini statistici, storici o scientifici. I c.d. "dati pseudonimi" sono quei dati personali che sono artificiosamente modificati negli elementi identificativi con elementi ulteriori e diversi e tali da rendere estremamente difficile l'identificazione dell'interessato (ciò obbliga chi tratta i dati pseudonimi di prevedere adeguate misure contro possibili abusi).

d) "**dati relativi alla salute**": qui dovrebbero ritenersi inclusi i dati personali riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso, ivi comprese le prestazioni di servizi di assistenza sanitaria che rivelino informazioni relative allo stato di salute.

2. Sui diritti degli interessati.

Il Gdpr introduce nuovi diritti a tutela dell'interessato; ciò in un'ottica di semplificazione delle procedure esperibili, adottando modalità organizzative finalizzate ad "***agevolare l'esercizio, da***

parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione" (cfr. "Considerando", n. 59):

1 diritto di revocare il consenso → (art. 7, paragrafo 3): "***L'interessato <u>ha il diritto di revocare il proprio consenso in qualsiasi momento</u>. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato***".

2 diritto di accesso → (art. 15) "***L'interessato ha il diritto di ottenere dal titolare di 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;

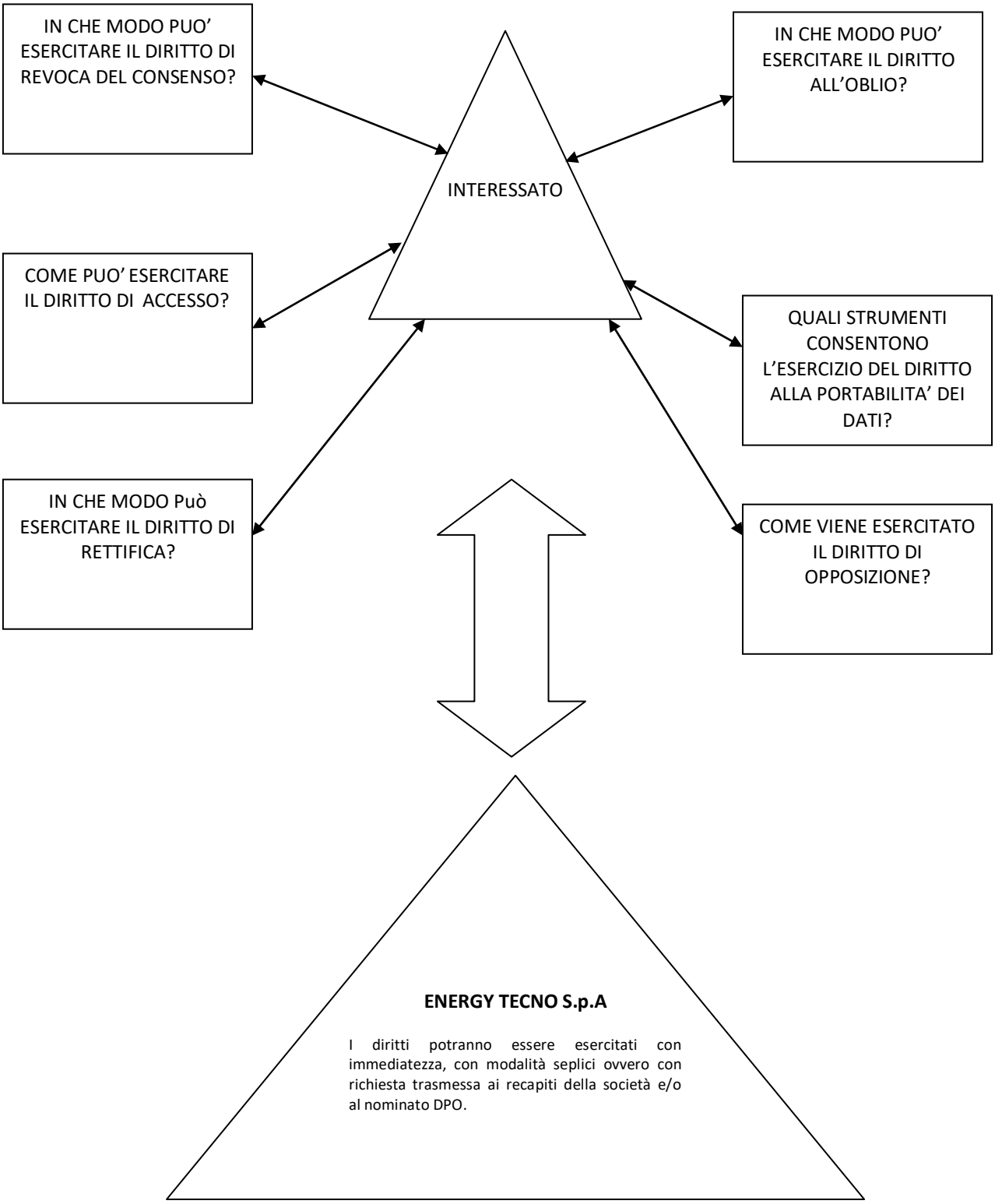
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

3 diritto di rettifica e di limitazione del trattamento → (art. 16) "*L'interessato ha il diritto d 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*".

per inviare la risposta definitiva, in caso di complessità della richiesta o di un eccessivo numero di domande pervenute). Si tratta di attività che (ove ritenute obbligatorie sulla base di alcuni indici) coinvolgono, inevitabilmente, benché in misura diversa, sia il "Titolare" che il "Responsabile", vale a dire, l'obbligo di redigere e conservare il "Registro del Titolare" e il "Registro del Responsabile" ed aventi ciascuno un preciso contenuto minimo.



3. Sulle sanzioni.

Il Gdpr inasprisce le sanzioni, stabilendo un tetto massimo significativamente più elevato di quello previsto con la previgente normativa. Ad esempio, per le violazioni degli obblighi del "Titolare" e del "Responsabile" (art. 25 e art. 32), la sanzione prevista può arrivare fino ad un aumento massimo di 10 milioni di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Invece, in caso di violazioni dei principi fondamentali in materia di protezione dei dati personali, dei diritti dell'interessato, per l'inosservanza degli ordini dell'autorità di controllo, il Regolamento lascia agli Stati membri la possibilità di prevedere sanzioni.

***

A tal proposito, il co. 13 dell'articolo 22 del D. Lgs. n. 101/2018 (c.d. «Decreto di armonizzazione») così precisa: «*Per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie*».

L'errata interpretazione di tale disposizione potrebbe condurre ad un equivoco: considerare gli otto mesi come una sorta di "proroga" (durante le sanzioni non verrebbero applicate).

Invece, onde voler scongiurare qualsiasi sanzione – ma soprattutto al fine di tutelare gli interessi degli Interessati che forniranno dati – la Energy Tecno S.p.A. è ben consapevole dell'impianto normativo introdotto con il Gdpr e, pertanto, pone (e porrà con sempre maggior consistenza) notevoli accorgimenti per meglio aderire allo spirito e alle prescrizioni delle nuove disposizioni.

4. Analisi e governance.

Il Gdpr adotta un nuovo approccio di analisi e *governance* del rischio: alla tutela rimediale, infatti, predilige un impianto di **sicurezza proattiva**, basato su strumenti a carattere preventivo e anticipartorio della tutela dei dati personali. Così, emerge un adempimento posto in capo al "Titolare" – che, quindi, è obbligatorio – allorquando il trattamento consiste:

1. nella valutazione sistematica e globale di aspetti personali relativi a soggetti, basata su un trattamento automatizzato e sulla quale si fondano decisioni che hanno effetti significativi;

2. un trattamento su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati;

3. una sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In tali casi, qualora dalla valutazione emerga un effettivo rischio il "Titolare" dovrà rivolgersi all'Autorità Garante della privacy al fine di avviare la consultazione preventiva.

5. (Segue) Ambito soggettivo: figure coinvolte nel processo di trattamento dei dati.

Il Gdpr, tra l'altro, individua espressamente i soggetti destinatari della normativa:

a) INTERESSATO → da intendersi il soggetto (persona fisica) identificato o identificabile e i cui dati sono oggetto di trattamento;

b) DESTINATARIO → ovvero ogni persona fisica o giuridica, autorità pubblica, servizio o altro organismo che riceve comunicazione di dati;

c) SOGGETTO TERZO → vale a dire la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il "Titolare", il "Responsabile" e la persona autorizzata al trattamento sotto l'autorità diretta del "Titolare" o del "Responsabile";

d) TITOLARE DEL TRATTAMENTO →da intendersi la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento dei dati personali. L'art. 26 Reg. 679/2016 prevede, altresì, la possibilità della contitolarità del trattamento. Giova precisare che il "Titolare" è obbligato a definire specificatamente – servendosi di atto giuridicamente vincolante – il rispettivo ambito ed i compiti gravanti sullo stesso, con particolare riguardo all'esercizio dei diritti degli interessati;

e) RESPONSABILE DEL TRATTAMENTO →ovvero la persona fisica o giuridica, l'autorità pubblica, il servizio o latro organismo che tratta dati personali per conto del "Titolare". Tra le parti (cioè tra "Titolare" e "Responsabile") deve formalizzarsi un contratto (o altro atto giuridico conforme al diritto dell'Unione) che disciplini tassativamente la matura, la durata e la finalità del trattamento nonché le categorie dei dati oggetto di trattamento le misure tecniche organizzative, etc.

interessati, ma, ancora, include **l'onere di rendicontare e dimostrare di aver adottato le misure tecniche ed organizzative adeguate per soddisfare gli standard di tutela richiesti dal Gdpr**. Peraltro, il principio di autoresponsabilizzazione deve interpretarsi quale unicum con gli altri principi di protezione dei dati fin dalla progettazione (privacy by design) e dell'ulteriore introdotto concetto della privacy by default. Non a caso, la valutazione di conformità dovrebbe essere effettuata dal "Titolare" "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento*" (cfr. art. 25)

- **PRINCIPOIO DELLA LIMITAZIONE DELLA FINALITA' →** i dati devono essere "***raccolti o finalità determinate, esplicite e legittime,*** *e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o ai fini statistici non è, conformemente all'art. 89, paragrafo 1, considerato compatibile con le finalità iniziali*". Il trascritto (art. 5, paragrafo 1, lett. b, Reg. 679/2016) enuncia il c.d. "principio della limitazione della finalità" per il quale è necessario che la finalità del trattamento dei dati personali debba essere precisata all'interessato al momento della raccolta. Nell'ipotesi di nuove (e diverse) finalità rispetto alla pregressa raccolta dei dati sarà necessario – anzi, obbligatorio – sottoporre nuovamente all'interessato una nuova informativa ed acquisendo la relativa (nuova) manifestazione del consenso.

- **PRINCIPIO DI MINIMIZZAZIONE DEI DATI →** i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. In maniera più asciutta il principio in parola risponde all'interrogativo: quali dati è possibile raccogliere? La risposata non può che essere del seguente tenore: possono essere raccolti solo i dati strettamente necessari all'esecuzione dell'incarico.

- **PRINCIPIO DELLA LIMITAZIONE DELLA CONSERVAZIONE →** i dati "***devono essere 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 ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica 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*" (rt. 5, paragrafo 1, lett. e) Reg. 679/2016). Ciò significa: - che i dati devono essere conservati per un periodo di tempo non superiore al conseguimento delle finalità per le quali sono trattati; - il

regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

Ancora, sullo stesso versante, le linee guida del "Gruppo art. 29" chiariscono che occorre tenere in debito conto, tra l'altro, di alcuni **indici/fattori**[17]:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Ciò significa, allora, in base all'articolo 37, paragrafo 1, lettere b) e c), del Gdpr, che il trattamento di dati personali (che, appunto, avviene su "larga scala") effettuato da Enegy Tecno S.p.A. farebbe scattare **l'obbligo di nomina di un RPD (o DPO)**.

Ciò premesso, allora, come di seguito meglio si dirà, la Enegy Tecno S.p.A. in qualità di "Titolare" **NOMINA** (si v. separato atto di "Conferimento dell'incarico", allegato alla presente relazione) la sig. **NOEMI CALOGIURI** (C.F.: CLGNMO79S47E506L – PEC: n[illegible]alogiuri@pec.it – dpoet@energytecno.com) quale **RESPONSABILE DELLA PROTEZIONE DATI** per conto di Energy tecno S.p.A. [si tratta di una nomina posteriore a partire dal mese maggio 2019. Essa si è resa necessaria per la sostituire la posizione del precedente DPO a suo tempo incaricato; cfr., separato atto di nomina]. **Chiaramente, incomberà sullo stesso nominato tutti le operazioni di cui al Gdpr, con particolare attenzione alle seguenti attività: tenuta dei registri delle attività di trattamento nonché valutazione d'impatto. Peraltro, incombe sempre sul nominato DPO la comunicazione di nomina la Garante (tramite notifica PEC).**

2. (Segue) In particolare sulla figura del DPO.

Questa figura è nominata dal "Titolare" o dal "Responsabile del trattamento". Il DPO ha principalmente la funzione di vigilare sull'applicazione delle norme sulla privacy da parte del "Titolare" o del "Responsabile". Inoltre, rappresenta un punto di contatto sia per gli interessati che per il Garante della privacy, con il quale il DPO è tenuto ad interfacciarsi.

Fuori dai casi in cui la nomina del DPO è obbligatoria (ossia, quando il trattamento è svolto da un soggetto pubblico/ quando il trattamento richiede un monitoraggio sistematico/ quando il

[17] Ivi, 10.

trattamento è effettuato su larga scala di particolari categorie di dati), **la nomina de DPO è facoltativa, ma può risultare consigliabile se la peculiarità di un trattamento lo suggeriscano**.

Pertanto, al fine di "classificare" la organizzazione di Energy Tecno attraverso alcune "catalogazioni" di sintesi, essa dovrebbe rapportarsi alle ipotesi sotto indiciate:

GRUPPO IMPRENDITORIALE	ART. 37 REG. 679/2016	FACOLTA' DI NOMINA DEL DPO DI GRUPPO
SOGGETTO PRIVATO CON MENO DI 250 DIPENDENTI	ART. 30 REG. 679/2016	ESCLUSIONE DI REGOLA DALL'OBBLIGO DI TENERE UN REGISTRO DEL TRATTAEMNTO DATI
SOGGETTO PRIVATO CON ATTIVITA' PREVALENTE MONITORAGGIO REGOALRE SU LARGA SCALA	ART. 37 REG. 679/2016	OBBLIGO DI NOMINA DI UN RESPONSABILE DELLA PROTEZIONE DATI (DPO)

La compilazione dei registri può essere eventualmente delegata – come in effetti la Energy Tecno delega con separato atto allegato alla presente – al DPO, (senza che ciò comporti uno spostamento della responsabilità che rimane comunque in capo al "Titolare" e al "Responsabile"). I registri devono essere redatti in forma scritta (anche elettronica) e deve essere periodicamente aggiornato; inoltre, su indicazione del Garante della privacy, i registri poc'anzi menzionati devono essere esibiti. Sono esonerate dal registro le imprese/organizzazioni con meno di 250 dipendenti, a condizione, però, che il trattamento dei dati non presenti rischi per i diritti e le libertà degli interessati.

Di tanto, come detto, si occuperà la nominata figura DPO, il dott. Fabio Cordella.

3. Report/scheda audit/test di autovalutazione iniziale.

a) Individuazione settori interessati al Gdpr

b) Individuazione soggetti incaricati di adeguare i processi, la modulistica, i procedimenti

c) Pianificazione raccolta informazioni

d) Pianificazione attività di valutazione dei rischi

e) Istituzione procedure per garantire che le violazioni dei dati siano rileate, segnalate e studiate

f) Pianificazione attività di valutazione di impatto privacy

g) Designazione Responsabile della protezione dei dati (DPO)

h) Valutazione legittimazione trattamento con consenso dell'interessato

i) Valutazione sistemi utilizzati raccolta consenso

j) Verifica informativa e sua conformità al Gdpr

k) Valutazione per procedure per fornire copie dei dati agli interessati che lo richiedono

l) Verifica dell'applicabilità della portabilità dei dati

m) Verifica dell'applicazione del diritto all'oblio

n) Valutazione per la realizzazione corsi per il pesonale per illustrare adempimenti previsti dal Gdpr

La scheda AUDIT – compilata e controfirmata – della Energy Tecno S.p.A è acclusa alla presente relazione e ne forma parte integrante.

4. Il contesto di Energy Tecno S.p.A. in relazione agli adempimenti del Gdpr.

Per quanto precede, allora, può ben dirsi che la Energy Tecno S.p.a. è soggetto "destinatario" (art. 4, punto 7, Reg. 679) della normativa, ovverossia inquadrabile quale persona giuridica che riceve comunicazione di dati personali e, come tale, obbligata a porre in essere tutti gli adempimenti necessari per assicurare la tutela dei dati.

Inoltre, la stessa Energy Tecno S.p.A. assume – secondo quanto previsto dal Gdpr – il ruolo (e la funzione) di "Titolare del trattamento" (art. 4, co.1, punto 7, Reg. 679); ciò significa, che essa diventa primario centro di responsabilità (dovendo dimostrare di avere adottato misure giuridiche, organizzative, tecniche per la protezione dei dati personali) dovendo revisionare e aggiornare l'informativa privacy da fornire agli interessati (peraltro, il Gdpr arricchisce il contenuto dell'informativa con ulteriori indicazioni che il "Titolare" deve fornire all'interessato, in modo trasparente e chiaro, ciò prima di procedere al trattamento).

In ordine al "Responsabile del trattamento" (art. 4, co. 1, punto 8, Reg.), vale a dire la persona (fisica o giuridica/autorità pubblica/servizio o altro organismo) che tratta dati personali per conto del "Titolare del trattamento", la Energy Tecno S.p.A. ha inteso designare – come già riferito – la sig. **NOEMI CALOGIURI** (C.F.: CLGNMO79S47E506L – PEC: n.calogiuri@pec.it – dpoet@energytecno.com) quale **RESPONSABILE DELLA PROTEZIONE DATI** per conto di Energy tecno S.p.A.

******

Pertanto, a seguito del conferito incarico di consulenza da parte dall'Amministratore Unico p.t. di Energy Tecno S.p.A., dopo un periodo di osservazione e dopo aver provveduto alla

somministrazione di test autovalutativi, con la presente si intende offrire le risultanze e una accurata disamina, di seguito si illustrano i punti di maggior interesse:

- la Energy Tecno S.p.A. ha dichiarato di trattare esclusivamente: “dati anagrafici”/ dati “iban”;
- la Energy Tecno S.p.A. ha dichiarato di trattare dati di: clienti/fornitori/dipendenti/collaboratori saltuari;
- la Energy Tecno S.p.A. ha dichiarato di comunicare a terzi sono i dati dei propri clienti e, invece, di non diffondere tali dati ad altri;
- la Energy Tecno S.p.A. ha dichiarato la limitata conservazione dei dati per un periodo che non supererà, quindi, i cinque anni;
- rispetto alla sicurezza informatica la Energy Tecno ha dichiarato l’utilizzo di apparecchiature elettroniche che, sebbene adeguate, richiedono alcuni accorgimenti per garantire una sufficiente protezione dei dati.

******

Tutto ciò premesso si indicano a titolo meramente esemplificativo (ma con un grado di incidenza fattiva per l’adeguamento) le **seguenti (necessarie) operazioni**:

1) NOMINA DPO (sarà il medesimo nominato ad effettuare le incombenze prescritte);
2) INDICARE RAPPORTI TRA TITOLARE E RESPONSABILE ESTERNO (altresì detto COTITOALRE) che tratta dati per conto della Energy Tecno S.p.A.;
3) ADEGUAMENTO NORMATIVO DELLA INFORMATIVA PRIVACY PER CLIENTI/DIPENDENTI/COLLABORATORI SALTUARI;
4) ADEGUAMENTO – con sempre maggior accortezza – LO SPAZIO FISICO DELL’ARCHIVIO CARTACEO AFFINCHE’ QUESTO SIA RISERVATO SOLO AL PERSONALE CHE PUO’ TRATTARE I DATI nonché METTERLO IN SICUREZZA (apponendo cartellonistica adeguata) e, poi, RENDERLO IMMUNE DA RICONOSCIMENTI DIRETTI (ogni fascicolo deve essere, ad es., indicato con un progressivo cronologico senza che si possa immediatamente cogliere il dato personale riferito e ivi contenuto);
5) FORMAZIONE DEL PERSONALE CHE TRATTA I DATI (con rilascio di certificazione) SULLE NORME COMPORTAMENTALI PER FAVORIRE IL RISPETTO DEL GDPR.

I soprarichiamati punti sono già in atto e, inoltre, la Energy Tecno S.p.A. provvede in corso d’opera ad effettuare quanto necessario.

******

In considerazione dell'attività prevalente della Energy Tecno S.p.A. e all'esito del periodo di osservazione, si consiglia:

6) EFFETTUARE NELL'ANNO ALMENO UNA DPIA (incombe al DPO);
7) EFFETTUARE UNA PROVA DI FORZA/TENUTA DEL SISTEMA INFORMATICO (cioè simulare un attacco informatico);
8) all'esito, EFFETTUARE UNA RICOGNIZIONE DEI DATABASE INFORAMATICI (se del caso ADEGUARE I SISTEMI OPERATIVI) e/o DISPORRE UNA CONSULENZA INFORMATICA (soprattutto per garantire: un backup dei dati ed implementare un archivio informatico/rendere i sistemi di accesso degli operatori più efficaci).

Lecce, 4 giugno 2019