SAGRES S.r.l.

MODELLO ORGANIZZATIVO PRIVACY
SAGRES S.r.l.

Il Modello Organizzativo Privacy di SAGRES S.r.l. è composto da una "Parte Prima" che illustra sinteticamente i contenuti del Regolamento UE 2016/679 e da una "Parte Seconda" che, unitamente agli allegati, costituiscono parte integrante del modello stesso.

PARTE PRIMA

IL REGOLAMENTO UE 2016/679

1. PRINCIPI GENERALI

Nel novellare la direttiva 95/46/CE, il Regolamento (UE) 2016/679 (di seguito anche "il Regolamento" o "GDPR") da un lato richiama principi ormai consolidati e stabili già presenti nel precedente testo normativo, dall'altro lato introduce novità non indifferenti che devono essere applicate al trattamento e prese in seria considerazione da chi svolge attività di trattamento.

I **principi cardine** alla base del trattamento dei dati personali sono da sempre:

- Principio di liceità, correttezza e trasparenza del trattamento nei confronti dell'interessato.

Liceità e correttezza: Il trattamento è lecito solo alle condizioni previste espressamente dall'art. 6 del Regolamento ovvero quando l'interessato ha espresso il proprio consenso (un consenso informato) al trattamento dei propri dati per una o più specifiche finalità, o quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte, o ancora quando il trattamento è necessario per adempiere un obbligo legale a cui è soggetto il titolare del trattamento. In fine il

trattamento è lecito quando lo stesso è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica ovvero quando è necessario per l'esecuzione di un compito di interesse pubblico o per il perseguimento del legittimo interesse del titolare del trattamento. Proprio a proposito di tale ultima situazione, è doveroso fare un bilanciamento tra gli interessi dei titolari del trattamento e gli interessi, i diritti e le libertà fondamentali degli interessati e può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.

Trasparenza: Oltre ad essere un principio fondamentale del trattamento, quello della trasparenza è anche un diritto dell'interessato. Devono essere trasparenti le modalità con cui sono raccolti e utilizzati i dati personali e devono essere facilmente accessibili e comprensibili le informazioni e comunicazioni relative al trattamento (identità del titolare del trattamento, finalità del trattamento, diritti degli interessati…).

- Principio di limitazione delle finalità dei dati: i dati personali devono essere raccolti per finalità determinate, esplicite e legittime e successivamente devono essere trattati in una modalità che sia compatibile con tali finalità. Il trattamento dei dati per finalità diverse da quelle per le quali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con tali iniziali finalità.
È poi possibile l'ulteriore trattamento ai fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici.

- Principio di minimizzazione dell'uso dei dati: i dati personali raccolti e trattati devono essere sempre adeguati, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati.

- Principio di esattezza dei dati: i dati personali devono essere sempre esatti e aggiornati. Eventuali inesattezze devono essere tempestivamente rettificate ovvero i dati inesatti devono essere cancellati.

- Principio della limitazione della conservazione: i dati personali devono essere conservati per il tempo necessario al raggiungimento delle finalità per le quali sono trattati.

Oltre ai principi già presenti nella disciplina previgente e sopra esposti, nuovo principio esplicitato dal Regolamento UE 2016/679 è quello dell'**integrità e della riservatezza**: i dati devono infatti essere sempre trattati in maniera da garantire una sicurezza adeguata, il che prevede l'adozione di misure di sicurezza tecniche ed organizzative adeguate per proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o dal danno accidentale.

L'art. 25 del Regolamento introduce poi i principi di **privacy by design** e **privacy by default**: la

protezione dei dati diventa essa stessa un principio cardine dal momento che deve essere prevista dal titolare fin dalla progettazione dei sistemi di trattamento dati. Il titolare deve poi preoccuparsi che, per impostazione predefinita, siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

Infine è da annoverare tra i nuovi principi del Regolamento quello della **responsabilità del titolare del trattamento**: tenuto conto della natura, contesto e finalità del trattamento nonché dei vari rischi che, a seconda del trattamento in questione, possono gravare su diritti e libertà delle persone fisiche, il titolare del trattamento deve garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento stesso.

2. I SOGGETTI E L'ONERE DELLA PROVA

Il Regolamento disciplina la **contitolarità** del trattamento (art. 26) e impone ai titolari, quando determinano congiuntamente le finalità e i mezzi del trattamento, di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti, con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente.
Vengono fissate in maniera più dettagliata (rispetto al Codice) le caratteristiche dell'atto con cui il titolare designa un **responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e 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.
Il Regolamento consente la nomina di **sub-responsabili** del trattamento da parte di un responsabile (art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3).
Sono previsti obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari.
Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un Responsabile della Protezione dei Dati (di seguito indicato anche con "Data Protection Officer" o "R.P.D." o "D.P.O.) (si segnalano, al riguardo, le linee-guida

in materia di responsabili della protezione dei dati recentemente adottate dal Gruppo di lavoro "Articolo 29"[1], qui disponibili: www.garante- privacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del Regolamento).
Anche il **responsabile non stabilito nell'Ue** dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.
Pur non prevedendo espressamente la figura dell' "**incaricato**" del trattamento (ex art. 30 Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a "**persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile**" (si veda, in particolare, art. 4, n. 10, del Regolamento).
Il Regolamento introduce un nuovo approccio, essenzialmente basato sulla **responsabilizzazione** del titolare del trattamento (si parla, infatti, di accountability e privacy "dimostrabile", in quanto l'**onere della prova** della conformità del trattamento grava sui titolari) e sul concetto di privacy by design. Il GDPR affida ai titolari il compito di individuare e predisporre autonomamente le modalità (incluse garanzie e limiti) più idonee per garantire il rispetto della normativa, attraverso un'analisi preventiva e specifica di tutti i trattamenti di dati effettuati, rinviando il controllo dell'Autorità Garante ad una fase eventuale e successiva.
Sarà ancora più centrale il ruolo dell'informativa sulla privacy rilasciata agli interessati, che andrà debitamente integrata per garantire il rispetto delle novità introdotte dal Regolamento: vanno ora indicati obbligatoriamente, ad esempio, anche il diritto dell'interessato di proporre reclamo all'autorità di controllo, il periodo di conservazione dei dati ed i dati di contatto del Data Protection Officer.
I titolari sono tenuti, ancora, a predisporre delle misure di sicurezza adeguate al rischio che il trattamento effettuato crea per i diritti e le libertà delle persone: si passerà, quindi, dalle misure di sicurezza statiche previste attualmente dall'All. B al Codice Privacy a delle misure di sicurezza definite in base alla valutazione dei rischi specifici esistenti e prevedibili in ciascuna realtà aziendale a seconda dei dati raccolti e delle attività di trattamento effettuate (l'art. 32 del GDPR contiene, infatti, una lista aperta e non esaustiva, perché la valutazione è rimessa caso per caso ai titolari).
Sarà, infine, compito dei titolari anche quello di disporre delle procedure idonee a rilevare e documentare in modo specifico e completo ogni eventuale **violazione dei dati personali** che si verificherà (**data breach**), informandone prontamente gli interessati e fornendo tutta la relativa documentazione al Garante, per l'accertamento di eventuali responsabilità.

3. IL MODELLO ORGANIZZATIVO PRIVACY

[1] Il Gruppo di lavoro "Articolo 29", istituito in virtù dell'articolo 29 della direttiva 95/46/CE, è l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata.

Il modello organizzativo persegue lo scopo di documentare la conformità della Società rispetto agli obblighi in materia di protezione dei dati personali gravanti sulla stessa in qualità di titolare del trattamento. Saranno parte integrante del modello organizzativo, tutte le misure tecniche ed organizzative adottate dalla società al fine di garantire e presidiare la sicurezza dei trattamenti dei dati personali.

L'organo deputato all'adozione ed alla predisposizione del modello organizzativo privacy è l'organo dirigente titolare del potere di amministrazione e controllo della società.

Il modello organizzativo privacy, per potere essere considerato uno strumento di governo della sicurezza dei trattamenti dei dati personali, deve essere efficace ed attuato efficacemente.

Tale modello **può ritenersi efficace** se:

- individua puntualmente, attraverso il registro dei trattamenti (art. 30 del GDPR) i trattamenti posti in essere dalla società nella sua articolazione funzionale, le diverse tipologie dei dati trattati, le categorie degli interessati coinvolti, le finalità del trattamento, le categorie dei destinatari, i termini di conservazione dei dati, le misure tecniche ed organizzative adottate;
- prevede specifici protocolli diretti a disciplinare i trattamenti dei dati da parte di tutto il personale a ciò preposto;
- prevede obblighi di informazione nei confronti del Team Privacy deputato a vigilare sul funzionamento e l'osservanza del modello;
- prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il modello organizzativo si considera attuato efficacemente quando prevede:

- una verifica periodica dello stesso modello e la sua modifica, sia quando si verificano violazioni delle prescrizioni, ovvero quando intervengano mutamenti nell'organizzazione, nell'attività della società o nel quadro normativo di riferimento;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Un'efficace applicazione del modello di organizzativo presuppone inoltre un'adeguata pubblicità all'interno della società ed a coloro che operano per conto della stessa, cosicchè tutti siano posti in grado di conoscere le procedure da seguire per un corretto svolgimento delle proprie mansioni.

4. RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (D.P.O.)

4.1. Soggetti obbligati alla designazione del D.P.O.

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati. Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).
Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di somministrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento (cfr. *Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, in aggiunta a quelle adottate dal Gruppo di lavoro Articolo 29 in Allegato alle Linee Guida sul RPD*).

4.2. D.P.O. interno o esterno

Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento UE 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.
Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del Regolamento; v. anche i punti 3.2 e 3.3. delle Linee Guida sopra richiamate).
I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento.

4.3. D.P.O. Persona fisica o Soggetto diverso

Il Regolamento (UE) 2016/679 prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del Regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.
Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (v. il punto 2.4 delle suddette Linee guida).

5. I REGISTRI DELLE ATTIVITÀ DI TRATTAMENTO

L'articolo 30 del GDPR prevede che:
1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione

internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate; d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

La predisposizione del Registro dei trattamenti non deve essere considerata alla stregua di un nuovo adempimento burocratico, ma come strumento che consente una gestione più efficace della data protection all'interno dell'azienda, oltre a rappresentare un elemento imprescindibile per l'individuazione e la realizzazione di un numero significativo di azioni inserite nell'Action Plan per l'adeguamento al GDPR. Difatti, tale nuovo adempimento consente alle singole organizzazioni di rispondere ad una pluralità di finalità, tra cui:

- tenere traccia delle operazioni di trattamento effettuate all'interno della singola organizzazione;
- costituire uno strumento operativo di lavoro mediante il quale censire in maniera ordinata le banche dati e gli altri elementi rilevanti per assicurare un efficace «ciclo di gestione» dei dati personali;
- dimostrare di aver adempiuto alle prescrizioni del Regolamento, nell'ottica del principio di "*accountability"*.

A conferma dell'opportunità generale di dotarsi del registro dei trattamenti, si possono considerare le raccomandazioni indicate nelle Linee Guida al regolamento, pubblicate dal Garante per la Protezione dei dati personali, in cui viene così espressamente previsto: "*la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali. Per tale motivo,* ***si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro*** *e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta*".

6. APPROCCIO BASATO SUL RISCHIO E DPIA (Data Protection Impact Assessment).

Il GDPR introduce il concetto della "responsabilizzazione" (accountability nell'accezione inglese) dei titolari e dei responsabili.
Ciò significa che i destinatari della normativa sono tenuti ad adottare comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la sua applicazione.
Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "*data protection by default and by design*" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 par. 1 del regolamento) e richiede, pertanto, **un'analisi preventiva e un impegno applicativo** da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**.
Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati; tali impatti dovranno essere analizzati attraverso un **apposito processo di valutazione** (si vedano artt. 35-36 GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.
All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale. L'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58 GDPR: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia successivo alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice Privacy italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da

parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia.
Dopo il 25 maggio 2018 cadranno altresì gli obblighi generalizzati di adozione delle cd. misure "minime" di sicurezza (ex art. 33 Codice Privacy) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati.
L'articolo 32 del GDPR si limita a suggerire una lista aperta, e non esaustiva, delle misure di sicurezza in astratto adottabili quali:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
In ossequio al princio della responsabilizzazione sarà in ultima istanza il titolare e/o il responsabile del trattamento a definire le misure più idonee a "garantire un livello di sicurezza adeguato al rischio" del trattamento.

7. LA COMUNICAZIONE AL GARANTE

L'articolo 33 del GDPR impone al titolare del trattamento di notificare all'autorità di controllo la **violazione di dati personali** (data breach).
Per "violazione di dati" si intende 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 (art. 4 par.12 GDPR).
La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.
L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche. Qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.
Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.
L'art. 33 par. 5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.
Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze

ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.
Il **termine per adempiere** alla **notifica** è brevissimo, settantadue ore dal momento in cui il titolare ne viene a conoscenza; l'**eventuale comunicazione agli interessati**, deve, invece, essere fatta senza indugio.
E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.
L'**eventuale ritardo nella notificazione** deve essere giustificato.
Il **mancato rispetto dell'obbligo** di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero:
- l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati); e
- la imposizione di sanzioni amministrative secondo l'art. 83 GDPR, il cui importo può arrivare a 10.000.000 di euro o al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
Occorre in ogni caso tenere conto che, la mancata notifica e/o comunicazione, possono rappresentare per l'autorità di controllo un indizio di carenze più profonde e strutturali quali ad esempio carenze od inadeguatezza di misure di sicurezza, in tal caso, trattandosi di ipotesi separate ed autonome, l'autorità procederà per l'ulteriore irrogazione di sanzioni.
Il rispetto degli obblighi di notifica (art. 33 GDPR) e di comunicazione (art. 34 GDPR), già in situazioni mediamente complesse in termini di dimensioni ed articolazione dell'organizzazione del titolare e/o in termini di numero di interessati di cui sono trattati i dati personali e/o in termini di operazioni di trattamento, o di quantità, varietà, natura dei dati trattati, richiede al Titolare di strutturare il trattamento dei dati personali avvalendosi di un sistema di conformità e gestione del rischio che preveda un sotto-sistema per la gestione degli incidenti e la continuità operativa.

8. RISARCIMENTO DEL DANNO E RESPONSABILITA'

L'articolo 82 del GDPR prevede espressamente che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere un risarcimento del danno da parte del Titolare o del Responsabile del trattamento.

Il **Titolare del trattamento** risponde per il danno cagionato dal suo trattamento che violi il GDPR.

Il **Responsabile del trattamento** risponde per il danno causato dal trattamento solo se non ha adempiuto agli obblighi del GDPR specificamente previsti per i responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti.

9. SANZIONI

Il GDPR disciplina le ipotesi per cui è prevista l'applicazione di sanzioni amministrative pecuniarie e/o penali.
Nonostante il GDPR focalizzi la propria attenzione, prevalentemente, sulle violazioni di tipo amministrativo, all'interno del Considerando 149 è stabilito che gli Stati Membri "dovrebbero poter stabilire disposizioni relative a sanzioni penali" come strumento di attuazione e tutela della nuova disciplina, pur sempre in ossequio al principio del ne bis in idem .
Per quanto riguarda le **sanzioni amministrative** esse possono raggiungere i 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di, a titolo esemplificativo:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'interessato;
- mancata o errata notificazione e/o comunicazione di un data breach all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza.

L'importo delle sanzioni amministrative pecuniarie può salire fino a 20 milioni di euro, o alternativamente, sino al 4% del fatturato mondiale dell'impresa nei casi di, a titolo esemplificativo:

- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito cross-border di dati personali ad un destinatario in un Paese terzo.

Il GDPR prevede un margine di discrezionalità circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa.
Di seguito alcuni criteri per la determinazione delle sanzioni amministrative pecuniarie, di cui all'articolo 83 paragrafo 2:

- "la natura, gravità e durata della violazione";
- "il carattere doloso o colposo della violazione";
- "il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi".

Con riferimento al primo criterio (natura, gravità e durata della violazione), lo stesso regolamento riconosce l'esistenza di diversi massimali per le sanzioni amministrative pecuniarie, i.e. 10 o 20 milioni di euro. Sarà, perciò, compito dell'Autorità nazionale competente valutare le circostanze di specie, alla luce di tali criteri generali, e poi decidere se procedere con una misura correttiva, più o meno severa, sotto forma di sanzione pecuniaria. All'interno del Considerando 148 è offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica". Anche tale inciso dimostra la tendenza del legislatore europeo di incoraggiare l'utilizzo delle sanzioni pecuniarie con un approccio "ponderato" ed "equilibrato". L'obiettivo ultimo rimane, infatti, quello di incentivare le società al rispetto della privacy by design e privacy by default, affidando lo strumento dell'applicazione di sanzioni pecuniarie così elevate, esclusivamente, al fine di reagire in maniera dissuasiva e proporzionata ad eventuali violazioni.

Con riferimento al secondo criterio, del carattere doloso o colposo della violazione, le valutazioni, circa l'esistenza di dolo o di colpa nella condotta, verranno effettuate sulla base di elementi oggettivi e sarà compito della giurisprudenza emergente definire ex ante "linee di demarcazione più chiare per valutare il carattere doloso di una violazione". Il Gruppo di lavoro "Articolo 29" ha, tuttavia, già provveduto ad esemplificare alcune condotte che potranno integrare il suddetto carattere doloso. Queste sono riconducibili alle ipotesi di:

- trattamenti illeciti autorizzati esplicitamente dal senior management, ovvero ignorando i pareri formulati dal DPO;
- modifica di dati personali, avente la finalità di fornire un'impressione "fuorviante" circa il conseguimento degli obiettivi individuati;
- vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Anche all'interno delle citate Linee Guida del Gruppo di lavoro "Articolo 29" viene, inoltre, precisato che la carenza di risorse economiche e materiali non potrà costituire ipotesi di esenzione di responsabilità. In funzione del cosiddetto risk based approach, infatti, il titolare dovrà progettare, sin dal principio, il proprio trattamento, stimando l'esistenza di possibili rischi per i diritti e le libertà degli interessati. Tale valutazione iniziale determinerà l'entità della responsabilità, in capo al Titolare o al suo Responsabile, tenendo in considerazione il contesto, le finalità e la natura del trattamento.

Con riferimento al terzo criterio, del grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi, il livello e l'entità della cooperazione con le autorità di controllo potrà costituire un fattore determinante, nella scelta di applicare o meno una sanzione amministrativa e, eventualmente, fissarne l'ammontare, qualora siano state limitate o azzerate le ripercussioni negative sui diritti degli interessati che si sarebbero altrimenti verificate in mancanza di tale collaborazione.

Il GDPR prevede, per quanto concerne le **sanzioni penali**, che "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento*" (considerando 149) e che "*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*" (art. 84 par. 1).

--oo0oo---

Una copia del testo del Regolamento UE 2016/679, delle Linee Guida sui Responsabili della Protezione dei Dati adottate dal Gruppo Art. 29 e delle Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato, vengono allegate al presente modello organizzativo (Allegato nr 1, nr 2 e nr 3).

10. LE ASSOCIAZIONI DI CATEGORIA

La Società è associata UNIREC Unione Nazionale Imprese a Tutela del Credito.
UNIREC assicura la professionalità, la correttezza e la trasparenza delle Associate a beneficio delle aziende committenti per prevenire i rischi reputazionali, richiedendo a tutti gli iscritti pieno rispetto di un rigido Codice Deontologico, che:
- interessa tutte le fasi e tutte le parti coinvolte nell'attività (aziende per la tutela del credito, aziende committenti e debitori);
- garantisce e disciplina le condizioni di onorabilità e professionalità delle Associate;
- i rapporti con gli Associati e con il Consiglio Direttivo;
- i rapporti con le aziende committenti;
- i rapporti con il debitore;
- i rapporti con i collaboratori e terzi.

La Società, poiché associata UNIREC, ha l'obbligo di uniformarsi alle norme previste dal Codice Deontologico, in difetto non potrebbe iscriversi o permanere in Associazione.
Il compito di vigilare sul pieno rispetto del Codice Deontologico e di tutti gli altri Regolamenti è affidato al Collegio dei Probiviri UNIREC.

UNIREC ha adottato inoltre precisi accordi deontologici sulle modalità di recupero con le principali Associazioni dei Consumatori.

Una copia del Codice Deontologico UNIREC viene allegata al presente modello organizzativo (Allegato nr 4).

PARTE SECONDA

IL MODELLO ORGANIZZATIVO PRIVACY DI SAGRES S.R.L.

SAGRES S.r.l. eroga diverse tipologie di servizi in ambito credit management, finance, contatct center e tributario.

1. IL MODELLO ORGANIZZATIVO PRIVACY DI SAGRES S.R.L.

L'Amministratore Unico di SAGRES S.r.l. ha deciso di adottare un modello di organizzazione privacy, per documentare la conformità della Società alle prescrizioni di legge in materia di protezione dei dati personali e segnatamente al Regolamento UE 2016/679.

Il modello di SAGRES S.r.l. è il risultato di una fase preliminare caratterizzata da un'attenta e minuziosa verifica della propria struttura.

L'elaborazione dello stesso ha consentito di verificare preventivamente le possibili aree a rischio nel trattamento dei dati personali ed attuare così i protocolli ed i presidi atti a garantire nel tempo il rispetto dei precetti contenuti nel GDPR da parte di chi lavora e/o collabora, a vario titolo, con SAGRES S.r.l..

Nella costruzione del modello, SAGRES S.r.l. ha tenuto conto sia di quanto previsto dalla normativa vigente, sia dalle Linee Guida fornite dal Gruppo di lavoro "Articolo 29" e dall'Autorità Garante della Protezione dei Dati Personali uniformandosi ad esse, ma nello stesso tempo adattondole alla realtà societaria.

1.1. Compiti dell'organo amministrativo

L'Amministratore Unico di SAGRES S.r.l. adotta il presente modello organizzativo e si assume il compito di verificarne sia l'aggiornamento, la diffusione e la conoscenza da parte di tutti coloro che operano nella Società sia, soprattutto, l' "efficacia" e l' "efficace attuazione" dello stesso, sia di apportare e deliberare tutte le modifiche del modello che si rendessero necessarie.

Nell'attuazione di tali compiti, L'Amministratore Unico è coaudiuvato:
- dal D.P.O.
- dall'Organismo di Vigilanza;
- dal Team Privacy, sotto definito.

Tali soggetti, a loro volta, sono coadiuvati dalle altre funzioni aziendali, che comunicano tutte le informazioni necessarie.

1.2. Finalità del modello di organizzazione

Tenendo conto dei precetti contenuti nel Regolamento UE 2016/679 e delle linee guida fornite dal Gruppo di lavoro "Articolo 29", dall'Autorità Garante della Protezione dei Dati Personali, nonchè di

tutta la normativa vigente, SAGRES S.r.l. ha deciso di adottare un modello organizzativo privacy al fine di:

- precisare a tutti coloro che operano in nome e per conto di SAGRES S.r.l. che la Società ha posto alla base di ogni trattamento di dati personali attuato nello svolgimento della propria attività, come elemento imprescindibile, il rispetto dei principi fondamentali elencati all'articolo 5 del GDPR;

- portare, quindi, a conoscenza di tutti coloro che operano in nome e per conto di SAGRES S.r.l. delle conseguenze per la stessa in termini di responsabilità del risarcimento dei danni e di sanzioni amministrative percuniarie/penali in caso di violazione del GDPR;

- precisare a tutti coloro che operano in nome e per conto di SAGRES S.r.l. le condotte che potrebbero realizzare le violazioni del GDPR;

- diffondere a tutti coloro che operano in nome e per conto di SAGRES S.r.l. la conoscenza delle procedure interne alla società, atte ad evitare le violazioni del GDPR;

- rendere noto a tutti coloro che operano in nome e per conto di SAGRES S.r.l. le sanzioni adottate dalla società nei confronti di chi non rispetta i principi enunciati dal Regolamento e la normativa vigente ad esso correlata.

2. FASE PRELIMINARE ALL'ADOZIONE DEL MODELLO ORGANIZZATIVO PRIVACY

Per la realizzazione del presente modello organizzativo, SAGRES S.r.l. ha da tempo avviato la seguente serie di attività preliminari.

2.1. Raccolta dei dati e dei documenti presenti nella società

a) elaborazione ed aggiornamento dell'organigramma societario;
b) identificazione dettagliata delle singole funzioni aziendali;
c) raccolta di tutta la documentazione esistente nella società quale, a titolo esemplificativo, procedure standard operative, informative, atti di designazione a Responsabile e/o Incaricato del trattamento, manuali operativi, contrattualistica, etc.;
d) individuazione delle policy, dei protocolli comportamentali e dei presidi societari;
e) identificazione del sistema sanzionatorio in vigore sia nei confronti dei dipendenti, sia nei confronti dei collaboratori.

2.2. Mappatura delle attività delle singole funzioni aziendali

Sulla base delle attività di cui ai precedenti punti, SAGRES S.r.l. ha quindi proceduto con l'individuazione dell'attività svolta in concreto dalle singole funzioni aziendali. Completano la mappatura le interviste a ciascun responsabile funzionale individuato, circa le mansioni da questi espletate oltre che dai soggetti a lui sottoposti.

E' stata pertanto creata una mappatura dettagliata che individua:
- i trattamenti posti in essere dalle singole funzioni aziendali;
- la coerenza tra gli atti di autorizzazione al trattamento ed i trattamenti realmente posti in essere da ciascun dipendente/collaboratore;
- le policy e/o procedure che disciplinano le attività poste in essere dalle singole funzioni aziendali;
- gli applicativi e gli archivi digitali e cartacei ove sono conservati i dati;
- le misure tecniche ed organizzative adottate per garantire la sicuerezza dei dati trattati;
- i soggetti interni ed esterni cui sono eventualmenti trasmessi i dati.

Tale mappatura ha consentito, dunque, una ricognizione minuziosa della struttura della società, tale da rendere più agevole l'eventuale identificazione di tutti i trattamenti posti in essere dalla società e di tutte le informazioni ad essi connessi.

La mappatura così realizzata si sostanzia nel Registro delle attività di trattamento ex articolo 30 del GDPR, ed è allegata al presente modello (Allegato n. 5).

2.3. Analisi del gap riscontrato

La mappatura delle funzioni aziendali e dei protocolli esistenti in SAGRES S.r.l. è stata, quindi, analizzata e per ogni singolo trattamento si è identificata l'eventuale mancanza di opportuni presidi.

Dalle carenze così individuate si è, quindi, proceduto ad elaborare nuovi e specifici protocolli finalizzati ad evitare il rischio di violazione del GDPR.

2.4 La revisione e l'integrazione delle misure tecniche – organizzative adottate dalla SAGRES S.r.l. per garantire la sicurezza dei dati personali

Le attività di cui ai punti precedenti hanno permesso di rivedere, aggiornare ed integrare le misure tecniche organizzative adottate dalla SAGRES S.r.l. al fine di grantire la sicurezza dei dati personali trattati.
In particolare sono stati aggiornate le seguenti protocolli comportamentali:

- amministrazione finanza e controllo cod 002
- acquisti con piccola cassa cod 002-01
- manuale della qualità

- modello organizzativo 231
- Procedura HR COD. HR003
- Procedura Car Policy COD. 003/01
- Procedura Sorveglianza e Sicurezza
- Codice Etico Aziendale
- Procedura AFC COD.002
- Procedura Commerciale cod. 7201 e 7501
- Istruzione Operativa 7501
- Procedura Rintraccio e Informazioni Commerciali COD.006B_01
- Procedura Servizi Postali
- Procedure Operative concordate con le Committenti
- Manuale Operativo " lawyer solution"

Sono state inoltre aggiornate le seguenti Procedure Operative:

Infine sono state adottate le seguenti nuove Policy:

- Policy Utilizzo Dati
- Policy Conservazione Dati;
- Policy Violazione dei dati personali (Data Brech) e registrazione degli eventi.

Sono, in ultimo, stati aggiornati tutti gli atti di Autorizzazione al trattamento e di designazione a Responsabile del trattamento coerentemente con i dati rilevati e contenuti nel registro dei trattamenti. Allo stesso modo sono state aggiornate tutte le informative ai sensi dell'articolo 13 GDPR utilizzate dalla società e tutte le clausole contrattuali utilizzate nei rapporti con i terzi.

2.5 Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

L'Amministratore Unico ritiene, in considerazione:

- delle analisi e valutazione dei rischi effettuate nell'ambito della predisposizione della Relazione sul Piano di Business Continuity e Disaster Recovery;
- delle misure di sicurezza tecniche adottate dalla Società ed indicate nel predetto documento, oltre a tutte le misure organizzative aggiornate ed integrate;
- del fatto che le attività in parola non hanno evidenziato rischi elevati, ai sensi dell'articolo 36 del GDPR;

che le misure complessivamente adottate dalla società sono in grado di garantire la sicurezza dei dati personali trattati (Allegati nr 6).

3. ADOZIONE DEL MODELLO ORGANIZZATIVO PRIVACY

Esaurita la fase preliminare poc'anzi illustrata, L'Amministratore Unico di SAGRES S.r.l. ha adottato il presente modello organizzativo.

Il Modello di SAGRES S.r.l. è composto da una "Prima Parte" che illustra sinteticamente i contenuti del Regolamento UE 2016/679 e da una "Parte Seconda" che, unitamente agli allegati che ne sono parte integrante:

- individua i trattamenti dei dati personali posti in essere dalle singole funzioni aziendali;
- accerta le coerenza degli atti di autorizzazione al trattamento conferiti ai singoli dipendenti/collaboratori;
- identifica le misure tecniche ed organizzative finalizzate a garantire la sicuerezza dei trattamenti dei dati personali;
- crea i presidi necessari alla prevenzione di eventuali violazioni del GDPR.

L'Amministratore Unico della Società si riserva il compito di adottare le modifiche, integrazioni ed aggiornamenti di carattere sostanziale ritenuti necessari per rendere efficace e per efficacemente attuare il modello organizzativo privacy.

Il compito di verificare la diffusione, applicazione ed i controlli sull'efficace attuazione del modello organizzativo compete all'organo amministrativo, al D.P.O. ed al Team Privacy.

4. DESTINATARI DEL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

I destinatari del modello organizzativo privacy di SAGRES S.r.l. sono tutti coloro che operano e/o collaborano con la società.

Più precisamente, il modello è destinato:
- a tutti i dipendenti/collaboratori autorizzati al trattamento dei dati ai sensi dell'articolo 29 del GDPR;
- a tutti i collaboratori esterni designati responsabili del trattamento ai sensi dell'articolo 28 del GDPR;
- a coloro che, a vario titolo, collaborano con SAGRES S.r.l. siano essi persone fisiche, o giuridiche.

Per tali soggetti si prevede l'inserimento nei contratti di apposite clausole che vincolino il permanere del rapporto al rispetto del modello organizzativo privacy.

5. NOMINA DEL D.P.O.

La SAGRES S.r.l. ha provveduto a designare l'avvocato Daniele Fiorelli della società ABCD S.r.l. D.P.O. esterno, ai sensi dell'articolo 37 del GDPR con atto notificato all'Autorità Garante della Protezione dei Dati Personali in data 24 maggio 2018.
Di seguito i dati di contatto del D.P.O.:

- email contatti.dpo@abcd.space

5.1. Funzioni assegnate al D.P.O.

La SAGRES S.r.l. ai sensi dell'articolo 38 del GDPR ha assegnato al D.P.O. le seguenti funzioni:

- 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 GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR, 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;
- fornire, quando richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo;
- 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.
La definizione delle funzioni del D.P.O. sono contenute nel contratto di servizi stipulato con ABCD S.r.l. in data 23 maggio 2018.

6. TEAM PRIVACY

6.1. Composizione, funzioni e funzionamento

Fanno parte del Team Privacy i responsabili delle seguenti funzioni aziendali:
- Dipartimento Legale
- Responsabile IT

come da funzionigramma allegato (Allegato nr 7).

Fatte salve le responsabilità del Titolare del Trattamento, il Team Privacy ha l'importante compito di coadiuvare il Titolare del trattamento ed il D.P.O. nell'attività di vigilanza sul funzionamento e sull'osservanza del modello organizzativo adottato dalla società, oltre che nel curare l'aggiornamento dello stesso.

In altri termini, tale Team ha la funzione di verificare nel quotidiano l'efficacia e l'effettiva attuazione del modello organizzativo nella società, a garanzia del mantenimento nel tempo di tali requisiti, mediante verifiche e, se necessario, anche proponendo aggiornamenti del modello stesso.

Il Team Privacy si riunisce almeno trimestralmente.
Partecipano alle riunioni del Team Privacy il Titolare del Trattamento nella persona del dott. Giacomo De Felice ed il D.P.O..
Nel corso di tali riunioni viene verificato lo stato di mantenimento del modello organizzativo e pianificate le eventuali azioni per apportare correttivi/aggiornamenti.
Delle riunioni del Team Privacy viene redatto processo verbale; quest'ultimo è conservato dal D.P.O o dal Titolare del trattamento.

Tutti i dipendenti/collaboratori autorizzati al trattamento ai sensi dell'articolo 29 del GDPR sono tenuti a segnalare ogni eventuale anomalia riscontrata o criticità relativa all'efficacia ed all'effettiva attuazione del modello direttamente al Team Privacy e/o al Titolare del trattamento e/o al D.P.O. (se nominato).

6.2. Flussi informativi nei confronti del D.P.O.

E' previsto un generale dovere di informazione nei confronti del D.P.O., onde consentire a quest'ultimo di operare ed assolvere alle funzioni assegnate, come peraltro previsto anche dal Regolamento UE 2016/679.

Il Team Privacy, in particolare, ha il compito di comunicare al D.P.O. :

- le variazioni all'organigramma societario che hanno un impatto sul personale autorizzato al trattamento, onde consentire le opportune valutazioni ed analisi;
- l'impiego di nuovi applicativi per lo svolgimento delle attività aziendali;
- la modifica delle misure teniche e/o organizzative adottate dalla società;
- condotte od operazioni poste in essere in violazione del presente modello organizzativo e più in generale delle regole interne in materia di protezione dei dati personali;
- ogni ipotesi di violazione dei dati personali trattati dalla SAGRES S.r.l. così come previsto dalla Policy Data Breach

È sanzionabile, su indicazione del D.P.O., il soggetto che, pur a conoscenza di informazioni, ometta di adempiere all'obbligo di segnalazione.

Il D.P.O., al fine di compiutamente realizzare le funzioni affidate, potrà comunque richiedere ed ha diritto di ottenere tutte le informazioni necessarie, prendere visione di documenti e consultare dati relativi alla Società.

6.3. D.P.I.A.

Laddove la Società dovesse decidere di effettuare nuovi trattamenti che prevedono l'adozione di nuove tecnologie, che possano, considerati la natura, l'oggetto, il contesto e le finalità, presentare rischi elevati per i diritti e le libertà delle persone fisiche, è fatto obbligo alla società, prima di procedere con al trattamento, di effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali.
In tali circostanze deve essere informato il D.P.O. affinchè possa coadiuvare la società nelle attività di valutazione in parola.

7. DIFFUSIONE DEL MODELLO ORGANIZZATIVO PRIVACY DI SAGRES S.R.L.

Perchè il modello organizzativo possa essere efficace ed efficacemente attuato è necessario che sia portato a conoscenza di tutti dipendenti e/o collaboratori, tenuti ad osservare con scrupolosa diligenza quanto ivi indicato.

Tutti vengono informati che il rispetto del modello organizzativo è condizione essenziale ed imprescindibile per il mantenimento dei rapporti con SAGRES S.r.l..

7.1. Personale/Collaboratori di SAGRES S.r.l..

Onde consentire una completa, accurata, accessibile e continua conoscenza, una copia del modello organizzativo, nonché i relativi allegati, viene messa a disposizione del personale e dei Collaboratori di SAGRES S.r.l. nella rete intranet aziendale/nella bacheca aziendale.

I dipendenti ed i collaboratori verranno preventivamente informati dell'adozione del presente modello organizzativo, nonché degli eventuali aggiornamenti adottati, mediante l'invio di apposite e-mail ed affissione di avvisi informativi nelle apposite bacheche societarie.

Dal momento che è importante una formazione adeguata nei confronti dei dipendenti e dei neo – assunti sui protocolli esistenti in azienda e sulle condotte da tenere nello svolgimento delle mansioni

affidate, vengono istituiti appositi corsi di formazione, necessari anche per illustrare i presidi adottati in materia di protezione dei dati personali trattati dalla società.
I momenti formativi vengono effettuati a cura del D.P.O..

Eventuali richieste di chiarimenti sui contenuti del modello organizzativo e del Regolamento UE 2016/679 potranno essere richiesti al D.P.O.. Il D.P.O. provvede quindi a rispondere alle richieste avanzate anche mediante l'invio di una e-mail collettiva.

7.2. Soggetti terzi

Il contenuto del modello di organizzazione, gestione e controllo dev'essere portato a conoscenza anche da tutti coloro che, direttamente o indirettamente, temporaneamente o stabilmente, instaurano e/o mantengono rapporti con SAGRES S.r.l.

Tali soggetti vengono informati dell'adozione del presente modello di organizzazione, gestione e controllo ed invitati a prendere conoscenza dei contenuti. A tal fine, si prevede che una copia del modello organizzativo venga immessa sul sito internet della società, in forma libera ed accessibile a chiunque.

8. SISTEMA DISCIPLINARE

L'efficace attuazione del modello organizzativo richiede l'adozione di un sistema disciplinare idoneo a sanzionare il mancato rispetto di quanto in esso previsto.

SAGRES S.r.l. pretende il rispetto e l'osservanza scrupolosa del modello organizzativo e delle procedure interne adottate e, più in generale, della normativa vigente.

Tale obbligo di ottemperanza altro non è che un dovere insito nel rapporto fiduciario che si instaura tra SAGRES S.r.l. ed il Personale e tutti coloro che svolgono attività per conto della società, con o senza rappresentanza.

In particolare:
- il Personale è tenuto a rispettare e ad uniformare la propria condotta al modello organizzativo privacy, anche in adempimento ai più generali obblighi di diligenza (art. 2104 c.c.) e di fedeltà (art. 2105 c.c.);

- i soggetti terzi (quali ad esempio fornitori, intermediari, collaboratori, etc.) sono tenuti a rispettare il modello organizzativo privacy in adempimento al dovere di diligenza e buona fede nell'esecuzione dei contratti intercorrenti con SAGRES S.r.l..

Eventuali violazioni di quanto previsto nel modello organizzativo sono considerate come lesive del rapporto di fiducia esistente tra SAGRES S.r.l. e l'autore della violazione, tanto da giusitificare l'adozione di appositi provvedimenti sanzionatori.

8.1. Sistema disciplinare nei confronti del Personale di SAGRES S.r.l..

Per quanto riguarda il Personale di SAGRES S.r.l. le sanzioni irrogabili sono attualmente quelle previste dalla legge e dal C.C.N.L. applicato in Azienda, nel pieno rispetto del procedimento disciplinare e sanzionatorio previsto dall'art. 7 della Legge n. 300 del 1970 (cd. Statuto dei Lavoratori), con le eventuali integrazioni del C.C.N.L..

In caso di violazione delle regole del modello organizzativo viene applicata la sanzione ritenuta adeguata e proporzionata all'inadempienza commessa, da individuarsi tra quelle previste dalla legge e dal C.C.N.L. di settore, nel rispetto del principio di adeguatezza e proporzionalità.

8.2. Sistema disciplinare nei confronti dei Soggetti terzi

Per quanto attiene i soggetti terzi che collaborano a vario titolo con SAGRES S.r.l. la mancata osservanza di quanto contenuto nel modello organizzativo potrà comportare, a seconda della gravità della condotta, la revoca per giusta causa o, in ogni caso, la risoluzione dei rapporti contrattuali intercorrenti, fatto comunque salvo il diritto al risarcimento del danno a favore di SAGRES S.r.l..

9. ALLEGATI

1) Testo integrale del Regolamento UE 2016/679;
2) Linee Guida sui Responsabili della Protezione dei Dati adottate dal Gruppo di lavoro Art. 29;
3) Nuove Faq sul Responsabile della Protezione dei Dati (RPD) in ambito privato;
4) Codice Deontologico UNIREC;
5) Registro delle attività di trattamento ex articolo 30 del GDPR;
6) Relazione sul Piano di Business Continuity e Disaster Recovery;
7) Funzionigramma relativo al Team Privacy.