REG PRY 00 Gruppo Veritas

Gestione degli adempimenti Privacy ai sensi del **Regolamento UE 679/2016 GDPR**

Conforme al Regolamento UE 679/2016 GDPR
Conforme alla norma UNI EN ISO 9001:2015
Conforme alla norma UNI EN ISO 14001:2015
Componente del Modello organizzativo ex dlgs 231/2001

VERITAS

Indice

1. Scopo 4
2. Campo di applicazione 4
3. Responsabilità 5
4. Definizioni 6
5. Regole per il trattamento dei dati 8
5.1 Modalità di trattamento e requisiti dei dati 8
5.2 Informativa sulla privacy all'interessato e consenso al trattamento dati 9
5.3 Comunicazione e diffusione dei dati personali 9
5.4 Trattamento dati sensibili 10
5.5 Trattamento dati giudiziari 10
5.6 Soggetti che effettuano il trattamento 10
5.7 Gestione documenti inerenti la privacy 12
5.8 Misure di sicurezza 12
5.8.1 Misure di sicurezza nei trattamenti senza l'ausilio di strumenti elettronici 13
5.9 Gestione di documenti e atti contenenti dati personali, sensibili o giudiziari 14
5.10 Gestione degli incidenti e Data Breach 14
5.11 Amministratore di sistema 15
5.12 Videosorveglianza 15
5.13 Geo-localizzazione 16
5.14 Centri di raccolta 17
5.15 Accesso alle sedi 17
6. Controllo e audit 17
7. Registro delle attività di Trattamento 18
8. Relazione Annuale sulla Privacy 18
9. Attivazione e/o modifica di Trattamento Dati 19
10. Diritti dell'interessato 19
11. Riferimenti normativi e documentali 21

preparazione	verifica	approvazione
Responsabile Gestione Dati Personali – Privacy *Mirco Simionato* (*FIRMATO*)	Direttore Risorse Umane e Organizzazione di Gruppo *Chiara Bellon* *(FIRMATO)*	Direttore Generale *Andrea Razzini* *(FIRMATO)*
	Responsabile Contenzioso Lavoro Disciplina Privacy Security *Laura Meggiorato* (*FIRMATO*)	Approvato dal CdA *18.04.2019*
	Responsabile Qualità Ambiente e Sicurezza *Giuliana Da Villa* (*FIRMATO*)	

VARIAZIONI: il documento è stato aggiornato al fine di recepire le recenti modifiche al contesto normativo di riferimento.

1. Scopo

Il Regolamento UE n. 679/20016 (GDPR) stabilisce i principi generali in materia di protezione dei dati personali.

Il contesto normativo di riferimento comprende inoltre l'ulteriore normativa primaria e secondaria in materia privacy e protezione dei Dati personali, compresi i provvedimenti emanati dal Garante, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

Il presente regolamento definisce le modalità di gestione dei dati personali in ambito aziendale allo scopo di:

- garantire che il trattamento dei dati personali detenuti da Veritas spa si svolga nel rispetto dei diritti di riservatezza e protezione degli stessi e in osservanza dei principi di proporzionalità, necessità, finalità e correttezza;
- stabilire modalità, termini e condizioni di gestione in osservanza di quanto sopra definito;
- garantire, ai fini della protezione dei dati personali detenuti da Veritas spa, che gli accessi ai sistemi informatici e agli archivi cartacei siano strutturati per assicurare un adeguato livello di riservatezza, conservazione, esattezza, correttezza, completezza, pertinenza e rintracciabilità delle informazioni ivi contenute.

Il contesto normativo di riferimento comprende inoltre l'ulteriore normativa primaria e secondaria in materia privacy e protezione dei Dati personali, compresi i provvedimenti emanati dal Garante, dalle Istituzioni europee e dal WP29, nonché le norme previste del codice civile e penale italiano.

2. Campo di applicazione

Il presente regolamento si applica a Veritas spa e, per quanto compatibile, a tutte le aziende del Gruppo Veritas e a tutte le attività che contemplano il trattamento di dati personali, comprese le attività affidate a terzi (attività affidate in *outsourcing*).

Veritas spa e le società del gruppo Veritas, debbono adottare il presente Regolamento attraverso una specifica deliberazione a cura dell'organo competente.

Il processo PRY Gestione risorse umane si compone di:

codice processo	descrizione processo	attività	documenti di riferimento
PRY	Gestione e controllo dati personali	Gestione dei rapporti con il garante della privacy	– **M PRY 30** Comunicazione data breach al Garante Privacy
		Redazione Registro dei Trattamenti e adempimenti conseguenti per Veritas, società controllate e partecipate 	– Regolamento degli adempimenti ai sensi del Regolamento UE 679/2016 GDPR - Gruppo Veritas – Registro trattamenti – **PR PRY 00** Valutazione e nomina responsabili esterni di trattamento dati personali ai sensi del Regolamento UE 679/2016 GDPR – Gruppo Veritas – **PR PRY 01** Gestione degli incidenti informatici e degli incidenti agli archivi cartacei. – **Informative** trattamento dati personali – **M PRY 31** Scheda rilevazione trattamento

3. Responsabilità

La tabella seguente descrive le attività che concorrono al raggiungimento degli obiettivi di processo e le relative responsabilità:

attività	referente
titolare dei dati personali e delle modalità di trattamento	Veritas S.p.A nella persona del legale rappresentante protempore, direttore generale/amministratore delegato della società/presidente
responsabili-referenti dei dati personali	dirigenti aree/responsabili
incaricati al trattamento	addetti incaricati presso le specifiche aree
amministratore di sistema (vedi profili di incarico)	responsabile/addetti sistemi informativi ed eventuali altri soggetti
analisi misure di sicurezza; elaborazione Registro trattamenti	ufficio Gestione dati personali privacy Veritas
rilevazione e gestione data breach	dipendenti aziendali, ufficio Gestione dati personali - privacy Veritas, ufficio Sistemi Informativi
definizione informative trattamento dati	ufficio Gestione dati personali privacy Veritas
definizione lettere d'incarico al trattamento dati (interne ed esterne all'azienda)	ufficio Gestione dati personali privacy Veritas
audit di controllo sull'osservanza in azienda delle disposizioni impartite nel GDPR e dalle procedure aziendali in materia	addetto Qualità e ambiente Veritas
responsabile del trattamento e archiviazione registrazioni provenienti dagli audit di controllo	addetto Qualità e ambiente Veritas
gestione dell'attività formativa *"autoformazione"* e della formazione in aula	ufficio Gestione dati personali - privacy di concerto con Risorse umane
formazione stagisti, cambi mansione e nuovi assunti	ufficio Gestione dati personali - privacy Veritas; addetto Qualità e ambiente di concerto
gestione informazioni/trasmissioni dati al garante	Legale rappresentante di concerto con DPO e ufficio Gestione dati personali - privacy Veritas
tenuta sotto controllo e aggiornamento delle informative (anche cartellonistica) relative alla privacy	ufficio gestione dati personali privacy Veritas responsabili-referenti
privacy impact assessment (PIA)	DPO, ufficio Gestione dati personali - privacy Veritas, sistemi informativi

4. Definizioni

Di seguito si precisa il significato delle principali definizioni tecniche utilizzate nel presente Regolamento (GDPR art. 4 e provvedimenti del Garante).

- **Garante** L'autorità in materia che viene eletta dalle camere; si tratta di un organo collegiale che opera in piena autonomia e con indipendenza di giudizio e di valutazione.
- **Trattamento** Qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti le raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
- **Dato personale** Qualunque informazione relativa a persona fisica, identificata od identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale
- **Dati identificativi** I dati personali che permettono l'identificazione diretta dell'interessato.
- **Dati sensibili** I dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale.
- **Dati giudiziari** I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del dpr 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
- **Dato anonimo** Il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.
- **Titolare** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- **Referente (ex Responsabile interno)** I soggetti interni alla realtà aziendale , preposti dal Titolare per vigilare sull'applicazione delle disposizioni in materia di protezione dei dati personali, vigilare sul rispetto delle misure di sicurezza, nominare gli incaricati, ecc.
- **Incaricati/Addetti Autorizzati** Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal referente.
- **Responsabile (ex Responsabile esterno)** La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali. Solitamente si tratta di un soggetto esterno a cui sono demandati dei trattamenti in outsourcing.
- **Responsabile della protezione dei dati personali (RPD/DPO)** La persona fisica che deve essere designata dal titolare del trattamento e dal responsabile del trattamento, in specifici casi (ad esempio, se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala)
- **Interessato** La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

- **Comunicazione** Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- **Diffusione** Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- **Blocco** La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
- **Banca di dati** Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
- **Sistema di autorizzazioni** L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo del richiedente.
- **Estremi identificativi** Si tratta del minimo insieme di dati identificativi utili a individuare il soggetto nell'ambito dell'organizzazione di appartenenza. In molti casi possono coincidere con nome, cognome, funzione o area organizzativa di appartenenza.
- **Amministratore di sistema** Le persone incaricate di gestire e mantenere i sistemi e gli impianti di elaborazione dati. L'attribuzione delle funzioni di amministratore di sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento di dati personali. La designazione ad amministratore è individuale e reca l'elencazione analitica degli ambiti di operatività in base al profilo di autorizzazione assegnato.
- **DPIA "Data Protection Impact Assessment" (GDPR art. 35)** Valutazione di impatto sulla protezione dei dati effettuata dal Titolare quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.
- **Data Breach/Violazione dei dati personali (GDPR art. 33)** 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.
- **Registro delle attività di trattameno (GDPR art. 30)** I Titolari e i Responsabili di trattamento devono tenere il Registro delle attività di trattamento svolte sotto la propria responsabilità, contenenti le informazioni di cui all'articolo 30del GDPR.

5. Regole per il trattamento dei dati

Per procedere alle operazioni di trattamento dati devono essere osservate le indicazioni riportate nei successivi paragrafi.

5.1 Modalità di trattamento e requisiti dei dati

Le operazioni di trattamento possono essere effettuate solo da incaricati che operino sotto la diretta autorità del titolare o del responsabile-referente del dato. Gli incaricati devono attenersi scrupolosamente alle procedure in materia impartite dalle società del Gruppo Veritas. Tali procedure, definite in ottemperanza al Regolamento UE 679/2016 (GDPR), vengono trasmesse agli incaricati attraverso specifica attività formativa in materia e, qualora necessario, con ulteriori eventuali comunicazioni scritte, (ad esempio il presente Regolamento, la pubblicazione Privacy Guida ad uso dei dipendenti, il Regolamento Informatico aziendale, specifiche comunicazioni aziendali ecc.).

Si sottolinea che gli incaricati sono da considerarsi tali qualora la loro designazione sia stata fatta per iscritto dal Titolare o dal responsabile-referente del dato oggetto di trattamento, e, solo qualora sia stato altresì designato l'ambito del trattamento loro consentito.

I dati personali oggetto di trattamento devono rispettare i seguenti requisiti di legge (GDPR – Art. 5):

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- 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;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

I dati non trattati secondo queste modalità e non aventi tali requisiti non possono essere utilizzati.

Riquadro 1

In particolare, devono essere adottate le cautele necessarie ad assicurare che il trattamento di dati personali sia effettuato solo ove ricorra almeno una delle seguenti condizioni:

- l'interessato ha espresso il proprio consenso;
- il trattamento è necessario per eseguire un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere ad un obbligo di legge;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per perseguire un legittimo interesse del titolare o di terzi, salvo che prevalgano gli interessi o i diritti e le libertà dell'interessato.

5.2 Informativa sulla privacy all'interessato e consenso al trattamento dati

Le operazioni di raccolta dati personali devono sempre essere svolte dopo aver dato informazione scritta od orale all'interessato circa Regolamento UE 679/2016 (GDPR):

- le finalità e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato (di cui agli articoli dal 15 al 22 del GDPR e al capitolo 9 del presente regolamento);
- gli estremi identificativi del titolare e se designato del responsabile della protezione dati (RPD/DPO) e le modalità attraverso le quali identificare e rintracciare i nominativi aggiornati dei responsabili per Veritas spa.

Qualora i dati personali non fossero raccolti in presenza dell'interessato, l'Informativa gli dovrà essere obbligatoriamente consegnata all'atto della registrazione dei dati stessi o trasmessa con la prima comunicazione utile.
Il trattamento dati personali da parte delle società del Gruppo Veritas è possibile solo con il consenso espresso da parte dell'interessato fatti salvi i casi espressamente previsti dalla legge (vedi riquadro 1).
Affinché il consenso abbia validità:

- deve essere riferito a uno specifico trattamento chiaramente individuato e deve essere documentato per iscritto;
- deve essere stata comunicata all'interessato la relativa Informativa al trattamento nei casi in cui debba essere acquisito il consenso;
- in caso di trattamento dati sensibili deve essere stato raccolto in forma scritta così come nei casi cui ci si avvalga dei dati di minori.

L'introduzione nel sistema di gestione di nuove informative sulla privacy, o modifiche alle informative esistenti, deve sempre essere concordata con l'ufficio Gestione dati personali – privacy di Gruppo.

5.3 Comunicazione e diffusione dei dati personali

Di norma, **non possono essere comunicati e diffusi dati per finalità differenti da quelle indicate nell'Informativa di trattamento**.
Ogni eventuale richiesta rivolta alle società del Gruppo Veritas da soggetti privati finalizzata ad ottenere informazioni sul trattamento, la diffusione e la comunicazione dei dati personali, anche contenuti in banche dati, deve essere formulata per iscritto e debitamente motivata. In essa debbono essere specificati gli estremi del richiedente e devono essere indicati i dati ai quali la richiesta si riferisce. La richiesta deve altresì indicare le norme di legge o regolamento che rappresentano il presupposto giuridico per la sua formulazione. Le richieste di comunicazione e di diffusione dei dati, provenienti da altri enti pubblici od amministrazioni, sono soddisfatte ai sensi di legge o di regolamento ovvero quando siano necessarie al perseguimento dei fini istituzionali del richiedente, che quest'ultimo avrà cura di indicare, o delle società del Gruppo Veritas.
Non è consentita la comunicazione e diffusione di dati sensibili, salvo che nei casi specificati dalla legge.
Sono escluse dai divieti sopra citati le richieste fatte alle società del Gruppo Veritas, purché siano conformi alla legge, da forze di polizia, autorità giudiziaria, organismi di informazione e sicurezza o da altri soggetti pubblici, per finalità di difesa, sicurezza dello Stato, prevenzione, accertamento o repressione di reati.

5.4 Trattamento dati sensibili

I dati sensibili (categorie particolari di dati personali) possono essere oggetto di trattamento solo con il **consenso scritto dell'interessato** (GDPR art. 9). Devono essere trattati nell'osservanza dei presupposti e dei limiti stabiliti dal codice in materia di trattamento dati personali e della legge (GDPR art. 9) e **non possono essere diffusi**.

Qualora sia necessario **per la gestione del rapporto di lavoro**, (anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza), adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria, tali dati possono essere oggetto di trattamento senza il consenso scritto da parte dell'interessato (GDPR art. 9).

I **dati sensibili** trattati dalle società del Gruppo Veritas sono:

- i dati idonei a rilevare lo stato di salute dei dipendenti trattati dall'area Servizio di sorveglianza sanitaria: tali dati non possono essere diffusi (GDPR art. 9);
- i dati inerenti le adesioni politiche e sindacali dei dipendenti trattati presso l'area Risorse umane e organizzazione di Gruppo.

5.5 Trattamento dati giudiziari

Il trattamento di dati giudiziari può avvenire soltanto sotto il controllo dell'autorità pubblica (GDPR art.10). Le disposizioni o provvedimenti in materia devono specificare:

- le rilevanti finalità di interesse pubblico del trattamento;
- i tipi di dati trattati;
- la tipologia di operazioni eseguibili.

I **dati giudiziari** trattati dalle società del Gruppo Veritas sono:

- i dati giudiziari di dipendenti, fornitori, esterni, aziende, società controllate, trattati presso le aree Affari legali e societari e Approvvigionamenti;
- i dati giudiziari raccolti in occasione di avvisi di selezione interna/esterna e relativi ai partecipanti alla selezione, trattati e detenuti presso la direzione Risorse umane e organizzazione di Gruppo.

5.6 Soggetti che effettuano il trattamento

In materia di trattamento dati personali il Regolamento UE 679/2016 (GDPR), raccordato con i Provvedimenti del Garante Privacy, individua le seguenti figure che operano con funzioni differenti nella gestione del dato personale dell'interessato:

- **titolare del trattamento** (GDPR art. 23 e 24) che con autonomia di potere decisionale esercita sulle finalità e sulle modalità del trattamento, compreso quanto concerne l'ambito della sicurezza. Il titolare ha facoltà di designare per iscritto eventuali responsabili di trattamento. Attraverso verifiche periodiche il titolare vigila sull'osservanza in azienda delle disposizioni impartite dal GDPR e dalle procedure aziendali in materia;
- **referente del trattamento (ex responsabile interno)** che, nell'ambito dei compiti affidatigli, analiticamente e per iscritto direttamente dal titolare, deve garantire il rispetto delle disposizioni vigenti in materia di trattamento dati, anche sotto il profilo della sicurezza. Per esigenze organizzative possono essere designati più responsabili/referenti di trattamento, anche mediante specifica suddivisione dei compiti. Il responsabile-referente, nell'esercitare i suoi compiti, deve attenersi alle istruzioni impartite dal titolare;
- **incaricati del trattamento/persone autorizzate al trattamento** che operano sotto la diretta autorità del titolare o del responsabile-referente, attenendosi alle istruzioni da loro impartite (attività for-

mativa, comunicazioni aziendali, procedure ecc.). La designazione degli incaricati e dell'ambito di trattamento loro consentito viene effettuata dal titolare o dal responsabile-referente **per iscritto.**

- **responsabile del trattamento (ex responsabile esterno)** (GDPR art. 28) qualora siano affidate in **outsourcing** attività di trattamento dati personali svolte in autonomia**. I soggetti esterni interessati al trattamento dati devono essere individuati dal referente aziendale del contratto, in fase di definizione dello stesso**. Le lettere d'incarico a tali soggetti vengono predisposte dall'ufficio Gestione dati personali – privacy di Veritas spa, sottoscritte dai soggetti terzi individuati, e inserite nella documentazione di affidamento. Per la gestione di tale attività è fondamentale il supporto della Direzione Approvvigionamento di Gruppo e degli uffici Approvvigionamento delle società del Gruppo Veritas, in particolare dell'area Approvvigionamenti beni e servizi, che trasmetterà all'ufficio Gestione dati personali – privacy tutte le informazioni utili alla predisposizione della lettera di nomina a responsabile esterno di trattamento dati (riferimenti societari ditta aggiudicatrice, oggetto dell'appalto, codice gara, codice CIG, data scadenza contratto ecc.), nonché copia del documento di affidamento perfezionato dal soggetto aggiudicatario. Per la descrizione di tali aspetti si rimanda alla procedura **PR PRY 00**.
- **amministratore di sistema** è colui che sovraintende alla gestione e alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico di cui è dotata la società. La nomina dell'amministratore di sistema deve avvenire, da parte del Titolare, previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati e in tema di sicurezza. La designazione dell'amministratore di sistema è individuale e deve recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Secondo la normativa vigente, l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.
- **responsabile della protezione dei dati (RPD/DPO)**

  Il GDPR prevede che il titolare del trattamento e/o il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati (GDPR art. 37, 38 e 39) ogniqualvolta:

  a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

  b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

  c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali.

  Inoltre il GDPR prevede che: "*un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento*".

  Il Gruppo Veritas, effettuando, per la natura dei servizi erogati, trattamenti su "larga scala" (es. gestione utenti servizio idrico; gestione contribuenti TARI/TARIP), ha definito di nominare un RPD/DPO esterno contattabile presso la sede legale della società in Santa Croce 489, 30135 Venezia (VE) - Mail: rpd@gruppoveritas.it - Pec: rpd@cert.gruppoveritas.it.

  Al responsabile della protezione dei dati RPD/DPO vengono affidati i seguenti principali compiti:

  - 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;
  - 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 e/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, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
- cooperare e fungere da punto di contatto con l'autorità di controllo (Garante Privacy);

5.7 Gestione documenti inerenti la privacy

Di norma i documenti, gli atti e le informative relativi alla privacy vengono predisposti, di concerto con gli uffici richiedenti, dall'ufficio Gestione dati personali – privacy che ne cura anche l'archiviazione.
Nell'eventualità che, per motivi di urgenza o di altra natura, debbano essere prodotti documenti inerenti la privacy da parte dei diversi uffici aziendali delle società del Gruppo Veritas, quali ad esempio informative lettere di nomina a incaricati o a responsabili esterni, ecc., copia di detta documentazione prodotta sarà trasmessa all'ufficio Gestione dati personali – privacy per opportuna conoscenza, verifica e archiviazione aziendale.
La modulistica inerente la privacy è disponibile sul portale aziendale Il Milione, nella sezione Sistema di gestione.

5.8 Misure di sicurezza

L'articolo 32, comma 1, del GDPR dispone che:
tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
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.
Per procedere al trattamento dei dati, il GDPR prevede, quindi, delle misure di sicurezza adeguate per garantire un livello di sicurezza rapportato al rischio.
Le misure di sicurezza devono, pertanto, essere definite per ogni trattamento a seconda del livello di rischio associato al trattamento stesso.
Per questo motivo nel registro dei trattamenti vengono riportate le misure di sicurezza previste per ogni trattamento.
A titolo indicativo le principali misure di sicurezza adottate dal Gruppo Veritas sono, attualmente, le seguenti:

Misure di Sicurezza Tecniche
- Controllo accessi con username e password
- Meccanismo automatico di allineamento tra HR e IT per la gestione delle utenze
- Piattaforma centralizzata di gestione dei privilegi di accesso (Active Directory)
- Utilizzo di differenti profili (i.e. lettura, scrittura, esecuzione) di accesso ai sistemi

- Utilizzo di utenze nominali
- Meccanismi di accesso sicuro da remoto
- Limitazione della lunghezza minima della password (i.e. 8 caratteri)
- Imposizione della sostituzione della password al primo accesso
- Blocco dell'accesso successivo a molteplici tentativi di accesso falliti
- Prevenzione del riutilizzo della password
- Tracciatura degli accessi e delle attività degli Amministratori di Sistema
- Utilizzo di protocolli di comunicazione sicura
- Procedure automatizzate di backup
- Esecuzione di test di ripristino dei backup
- Adozione di sito di Disaster Recovery
- Meccanismi automatizzati di applicazione degli aggiornamenti
- Adozione di software antivirus
- Misure di sicurezza di rete perimetrali e di segregazione della rete interna
- Conservazione sicura dei documenti cartacei
- Piattaforma centralizzata di gestione dei dispositivi mobili (MDM)

Misure di Sicurezza Organizzaztive

- Processo di valutazione delle capacità degli Amministratori di Sistema
- Elenco aggiornato degli Amministratori di Sistema
- Lettere di nomina ad Amministratore di Sistema
- Procedura per l'aggiornamento dell'elenco degli Amministratori di Sistema
- Processo di revisione periodica delle utenze da parte dei responsabili
- Processo di Patch Management
- Linee guida di corretto utilizzo degli strumenti informatici
- Istruzioni operative per la gestione degli incidenti di sicurezza informatica
- Piano di continuità operativa
- Procedura per l'esecuzione periodica di analisi dei rischi IT e Business Impact Assessment
- Linee guida di corretto utilizzo dei supporti cartacei
- Programmi di sensibilizzazione periodica in ambito sicurezza informatica
- Esecuzione di audit periodici in ambito sicurezza informatica

Ulteriore misura di sicurezza risulta essere l'adozione del Regolamento Informatico del Gruppo Veritas per i trattamenti effettuati con strumenti elettronici.

5.8.1 Misure di sicurezza nei trattamenti senza l'ausilio di strumenti elettronici

Il trattamento di dati personali senza l'ausilio di strumenti elettronici è consentito solo qualora siano adottate le seguenti misure minime di sicurezza:

- **aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative**: gli ambiti di trattamento consentiti ai singoli incaricati vengono periodicamente aggiornati e verificati con cadenza almeno annuale. La lista degli incaricati è redatta per dipendente e relativa specifica autorizzazione al trattamento. La raccolta e l'elaborazione di tali informazioni, utilizzate anche per l'aggiornamento del Registro dei Trattamenti, sono a cura dell'ufficio Gestione dati personali – privacy. È cura invece del titolare/responsabile-referente d'area d'individuare e trasmettere a tale funzione le informazioni relative ai trattamenti svolti nell'area di loro competenza;
- **adozione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti**: gli incaricati sono informati (corso di auto formazione on-line e distribuzione della presente procedura) circa le modalità di controllo e custodia dei documenti contenenti dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento (vedi paragrafo 5.9 Gestione di documenti e atti contenenti dati personali, sensibili o giudiziari).
  È responsabilità del titolare/responsabile-referente di formare gli incaricati sulla corretta custodia docu-

mentale;

- **adozione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati**: gli archivi aziendali che richiedono accesso selezionato sono quelli presenti negli uffici del Servizio di sorveglianza sanitaria dove sono state adottate idonee misure di custodia e controllo degli accessi come la chiusura a chiave delle stanze e degli armadi e l'utilizzo delle chiavi di accesso in carico esclusivamente al responsabile-referente e al suo incaricato.

5.9 Gestione di documenti e atti contenenti dati personali, sensibili o giudiziari

I documenti cartacei trattanti dati personali, sensibili o giudiziari non devono essere lasciati incustoditi o trasportati al di fuori delle sedi aziendali senza autorizzazione del titolare o responsabile-referente del trattamento. Particolare attenzione va posta inoltre nel caso in cui tali dati siano in unica copia.
Per il trattamento di atti e documenti contenenti dati sensibili o giudiziari è necessario che i medesimi siano controllati e custoditi dagli incaricati sino al termine delle operazioni per le quali sono stati loro affidati, in maniera tale che a essi non possano accedere persone prive di autorizzazione.
L'archiviazione di tali documenti deve essere effettuata:

- con sistematicità alla fine delle operazioni per cui sono stati trattati i dati;
- con un metodo che ne renda possibile una veloce rintracciabilità, anche al fine di poter garantire i diritti dell'interessato;
- in luoghi sicuri e adeguati al grado di riservatezza dei dati trattati, (ad esempio in armadi e cassetti chiusi a chiave). L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato.

Per quanto riguarda il trattamenti di atti e documenti contenenti dati sensibili o giudiziari è necessario che i medesimi siano controllati e custoditi dagli incaricati sino al termine delle operazioni per le quali sono stati loro affidati, in maniera tale che a essi non possano accedere persone prive di autorizzazione.

5.10 Gestione degli incidenti e Data Breach

Qualora si verifichino perdite, diffusioni non consentite o accessi non autorizzati di dati personali ogni dipendente del Gruppo Veritas dovrà immediatamente informare il proprio Responsabile diretto ed attenersi a quanto previsto nell'apposita procedura **PR PRY 01** di gestione degli incidenti informatici e degli incidenti agli archivi cartacei.
Nel caso in cui si verifichi una violazione dei Dati personali (Data Breach) che presenti un rischio per le libertà e i diritti degli interessati, il Titolare prevede una modalità immediata di reazione che permetta:

- la notifica dell'avvenuta violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza e, se ricorrono i presupposti, all'interessato (**M PRY 30** Comunicazione data breach al Garante Privacy);
- l'adozione delle misure necessarie ad attenuare gli effetti negativi della violazione.

Il Titolare tiene un registro degli incidenti, definito da apposita procedura che stabilisce le modalità interne che disciplinano il suo aggiornamento al sussistere di ogni violazione, indifferentemente dal rischio presentato per i diritti e le libertà degli interessati e meccanismi di conservazione di tutte le comunicazioni riguardanti la violazione. In tale registro sono indicati tutti gli elementi richiesti dalla normativa applicabile, tra cui:

- le circostanze relative all'incidente e/o alla violazione;
- le conseguenze;
- le misure adottate per contrastare l'incidente e/o limitarne gli effetti;
- i Dati personali coinvolti;

- informazioni adeguate per permettere al Titolare di determinare le motivazioni per avere o non aver effettuato la notifica al Garante.

Il processo di gestione degli incidenti e Data Breach è dettagliato nell'apposita procedura PR PRY 01, già sopra richiamata.

5.11 Amministratore di sistema

Per **Amministratore di Sistema** si intende quella figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza qualora questi consentano di intervenire su dati personali. Si tratta pertanto di operatori dotati di specifici privilegi informatici, che nello svolgimento delle loro consuete attività possono essere concretamente "responsabili" di specifiche fasi lavorative, le quali possono comportare elevate criticità rispetto alla protezione dei dati personali. Tali attività vanno considerate come trattamento di dati personali, anche se le informazioni accessibili non sono consultabili "in chiaro".

Non sono considerati invece Amministratori di Sistema tutti quei soggetti che solo occasionalmente intervengono sui sistemi di elaborazione e sui sistemi software, ad esempio per scopi di manutenzione a seguito di guasti o malfunzionamenti.

Le misure di sicurezza e gli accorgimenti adottati dalle società del Gruppo Veritas relativamente alla definizione e alle funzioni assegnate alla figura in oggetto sono le seguenti:

- la funzione di Amministratore di Sistema è attribuita, a seguito di valutazione fatta dall'area Risorse Umane e Organizzazione, a personale qualificato in grado di garantire il rispetto delle vigenti disposizioni in materia di trattamento dati, ivi compreso il profilo relativo alla sicurezza. Tale designazione è individuale e riporta l'elenco analitico degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato (vedi specifici profili professionali);
- all'atto della designazione di un Amministratore di Sistema viene fatta un'elencazione analitica degli ambiti di operatività a esso consentiti in base al profilo di autorizzazione assegnato;
- nel *Documento annuale di rendicontazione sulla privacy* sono riportati gli estremi identificativi aggiornati degli Amministratori di sistema incaricati;
- da parte degli Amministratori di Sistema sono stati adottati sistemi di autenticazione informatica ai sistemi di elaborazione e agli archivi elettronici (registrazione degli accessi logici). Tali tipi di registrazioni comprendono i riferimenti temporali e la descrizione dell'evento che le ha generate e vengono conservate per un periodo non inferiore a sei mesi;
- per i servizi di Amministratori di Sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

Tali misure di sicurezza e accorgimenti sono stati adottati in riferimento a quanto definito dal provvedimento del 27 novembre 2008.

5.12 Videosorveglianza

Nell'installazione e gestione di impianti di videosorveglianza presso le sedi dell'azienda devono essere osservate le indicazioni del Garante privacy, di cui al **provvedimento in materia di videosorveglianza dell'8 aprile 2010**, e quando previsto nell'accordo sindacale di Gruppo sulla videosorveglianza siglato in data.

In merito ai sistemi di videosorveglianza, per ottemperare alle disposizioni in termini di privacy, sono attualmente previste le seguenti condizioni:

- stipula di apposito accordo sindacale con le OO.SS. dei CCNL applicati in azienda ex art. 4 legge 300/70 ovvero presentazione istanza all'Ispettorato del lavoro competente (in Veritas è stato stipulato con le OO.SS., in data 12.09.2018, l'accordo quadro sulla videosorveglianza);
- i dati raccolti devono rispettare il principio di pertinenza e di non eccedenza, cioè vengono registrate solo le immagini strettamente necessarie a perseguire gli obiettivi di tutela della sicurezza e dell'incolumità del patrimonio e delle persone;
- l'accesso alle registrazioni è previsto solo per il personale appositamente incaricato, come previsto dall'accordo sindacale del 12/09/2018 (accordo quadro sulla videosorveglianza);
- la visualizzazione delle registrazioni avviene solo ed esclusivamente per verificare fatti anomali inerenti la sicurezza;
- il trattamento dei dati avviene secondo correttezza e solo per ragioni di sicurezza e tutela del patrimonio e incolumità delle persone (le immagini non possono essere utilizzate per finalità differenti);
- in caso di registrazione, il periodo di conservazione delle immagini deve essere limitato al massimo a 24 ore, fatte salve speciali esigenze di ulteriore conservazione in relazione a indagini (in Veritas tale limite di 24 ore è stato portato a 7 giorni a seguito delle criticità riscontrate nella gestione degli impianti di videosorveglianza e recepite nell'accordo quadro del 12/09/2018);
- di ogni nuova installazione e/o modifica di sistemi di videosorveglianza deve essere data tempestiva comunicazione all'ufficio Gestione dati personali – privacy;
- i sistemi di videosorveglianza installati in azienda devono essere segnalati da uno specifico cartello informativo, sulla base del modello elaborato dal Garante privacy, posto in prossimità di ogni singola telecamera.

5.13 Geo-localizzazione

Nell'installazione e gestione di impianti di geo - localizzazione su mezzi e/o dispositivi aziendali, devono essere osservate le indicazioni del Garante privacy, di cui al provvedimento in materia di geo-localizzazione del 4 ottobre 2011.

In merito ai sistemi di geo-localizzazione, per ottemperare alle disposizioni in termini di privacy, sono attualmente previste le seguenti condizioni:

- stipula di apposito accordo sindacale con le OO.SS. dei CCNL applicati in azienda ex art. 4 legge 300/70, ovvero presentazione istanza all'Ispettorato del lavoro competente (in Veritas sono stati stipulati con le OO.SS. gli accordi del 06/11/2007 per le barche aziendali, del 14/02/2013 per le autovetture, del 30/10/2009, 04/05/2010, 16/07/2013 per gli automezzi per la raccolta, del 13/12/2013 per i siti di disinfestazione e derattizzazione, del 14/01/2013 per i recapiti postali, del 18/09/2013 per le registrazioni del call-center);
- eventuale nomina di responsabile esterno del trattamento dati se il sistema di rilevazione dati è gestito presso terzi;
- ricognizione e nomina degli incaricati abilitati a collegarsi e a operare sul sistema;
- i dati raccolti devono rispettare il principio di pertinenza e di non eccedenza, pertanto la posizione dei mezzi o dei dispositivi non deve venire monitorata continuamente;
- definizione di tempi di conservazione dei dati trattati (indicati-

vamente non superiore a 90 giorni);

- ogni nuova installazione e/o modifica di sistemi di geo-localizzazione deve essere tempestivamente comunicata all'ufficio Gestione dati personali – privacy;
- dev'essere predisposta idonea Informativa estesa per i dipendenti
- si dovranno anche collocare all'interno dei veicoli vetrofanie recanti la dizione "VEICOLO SOTTOPOSTO A LOCALIZZAZIONE" o comunque avvisi ben visibili che segnalino la circostanza della geo-localizzazione del veicolo, anche avvalendosi del seguente modello elaborato dal garante Privacy.

5.14 Centri di raccolta

Nella conduzione dei centri di raccolta devono essere osservate le regole per il corretto trattamento dei dati personali così come previsto dalla "Informativa sul trattamento dei dati personali acquisiti con conferimento di materiali nei centri di raccolta", (**M PRY 03**). Tale informativa è disponibile presso tutti i centri di raccolta.
Per quanto attiene all'accettazione dei rifiuti di apparecchiature elettriche ed elettroniche (RAEE) dovrà essere compilato il modulo **M ECO 09** *"Conferimento di particolari tipologie di RAEE"*. Per il conferimento presso i Centri di Raccolta di materiale derivante da piccoli lavori di manutenzione e ristrutturazione domestica, è invece prevista la compilazione del modulo **M ECO 08** *"Conferimento materiale proveniente da piccoli lavori di manutenzione e ristrutturazione domestica"*.

5.15 Accesso alle sedi

Per motivi di sicurezza, sia propriamente delle persone fisiche, che di tutela delle informazioni, dei dati personali e del patrimonio aziendale, l'accesso alle sedi aziendali da parte di persone esterne (visitatori, fornitori, ecc.) deve venire appositamente registrato secondo le modalità previste dalla procedura **PR LOG 00**, attualmente in aggiornamento. Il corretto trattamento dei dati personali raccolti è descritto nell'apposita informativa **M PRY 07**.

6. Controllo e audit

Le misure di sicurezza, organizzative, fisiche e logiche da adottare per il trattamento dei dati personali sono delineate nel Registro delle attività di Trattamento e nella rendicontazione annuale sulla privacy. Quest'ultimo documento viene aggiornato annualmente a cura dell'ufficio Gestione dati personali- privacy e riguarda tutte le attività gestite dalle società del Gruppo Veritas concernenti tale materia, comprese quelle affidate a fornitori esterni.
L'area Qualità ambiente e sicurezza effettua audit di controllo atti a verificare l'effettiva adozione e applicazione delle misure di sicurezza previste e del complesso di operazioni concernenti il trattamento dei dati personali. I punti di controllo delle verifiche sono definiti e aggiornati in ottemperanza a quanto previsto dal GDPR e dai provvedimenti del Garante Privacy, qualora essi siano applicabili alla realtà aziendale.
Con cadenza semestrale l'area Qualità ambiente e sicurezza, inoltre, effettua verifiche circa l'operato degli Amministratori di Sistema secondo quanto previsto dal provvedimento del 27.11.2008 (punto 4.4 Verifica delle attività).
Obiettivo di questi audit è:

- verificare che l'Amministratore di Sistema svolga le sua attività nell'esercizio delle sue funzioni;
- verificare che l'Amministratore di Sistema svolga le sua attività conformemente alle mansioni attribuite, ivi compreso il profilo relativo alla sicurezza.

Le risultanza degli audit, oltre che ai referenti dell'area verificata, vengono trasmesse anche all'ufficio Gestio-

ne dati personali – privacy che le utilizza per aggiornare lo stato delle informazioni in materia in suo possesso.

7. Registro delle attività di Trattamento

Ogni titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità (Articolo 30 del GDPR).

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto del Titolare del trattamento e dell'eventuale RPD/DPO;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato che, per il Gruppo Veritas è identificato nell'Ufficio gestione dati personali - privacy.

Ciascun responsabile-referente di trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto alla tenuta del registro ogni elemento necessario alla regolare tenuta ed aggiornamento del registro stesso.

L'aggiornamento del registro avviene in continuo, inserendo ed aggiornando i trattamenti come indicato nel successivo Capitolo 9.

I nuovi incaricati, così come le cessazioni dall'incarico di trattamento dati, verranno individuati mediante le comunicazioni dell'area Risorse umane e organizzazione di gruppo sulla movimentazione del personale e mediante la verifica dei dati presenti negli aggiornamenti della struttura organizzativa. Attraverso queste modalità operative verranno perfezionate, in tempo reale, le lettere di nomina degli incaricati che verranno sottoposte all'accettazione da parte degli stessi e alla conseguente archiviazione.

Periodicamente, almeno una volta all'anno, l'Ufficio gestione dati personale – privacy effettuerà dei controlli assieme ai responsabili-referenti per verificare lo stato di aggiornamento dei loro trattamenti e delle loro nomine degli incaricati.

8. Relazione Annuale sulla Privacy

Prima dell'approvazione del Bilancio annuale, l'azienda predispone un relazione/rendicontazione annuale sulla privacy.

La relazione/rendicontazione annuale sulla privacy viene predisposta e approvata dal CdA delle società del Gruppo Veritas (entro il 31 marzo di ogni anno per Veritas, entro il 31 maggio di ogni anno per le altre società del Gruppo). Per la redazione di tale documento il Titolare dei dati delle società del Gruppo Veritas nomina un responsabile aziendale che si occupa di raccogliere tutte le informazioni idonee alla compilazione del documento in oggetto.

Tale responsabile aziendale risulta, attualmente, in capo all'ufficio Gestione dati personali – privacy.

Nello specifico il documento annuale riporta:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

- l'analisi dei rischi che gravano sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure di sicurezza in caso di trattamenti di dati personali affidati all'esterno;
- l'indicazione degli incidenti e dei data breach registrati durante l'anno;
- l'indicazione delle richieste prevenute da parte dagli interessati;
- eventuali altre informazioni o fatti, avventi durante l'anno, di particolare importanza ai fini della privacy;
- schede di sintesi sullo stato ed organizzazione dei sistemi informatici utilizzati dall'azienda;
- i riferimenti degli Amministratori di Sistema (interni ed esterni);
- nota finale con valutazioni ed indicazioni da parte del RPD/DPO dell'azienda.

L'ufficio Gestione dati personali – privacy, incaricato per l'elaborazione del documento di cui sopra, per la predisposizione dello stesso, richiede annualmente all'ufficio Sistemi informativi l'aggiornamento dei dati del sistema informatico e agli altri uffici aziendali qualsiasi ulteriore dato utile alla stesura del documento.

9. Attivazione e/o modifica di Trattamento Dati

L'attivazione di un nuovo trattamento, così come la modifica delle caratteristiche di un trattamento già in essere (nuovi dati da acquisire, nuove finalità, ulteriori modalità di trattamento rispetto a quelle inizialmente previste, ecc.) deve portare:

- all'aggiornamento del registro dei trattamenti;
- alla definizione della durata del trattamento;
- alla predisposizione/aggiornamento dell'informativa;
- alla ricognizione dei soggetti autorizzati al trattamento (incaricati) ed alla loro nomina;
- alle considerazioni sulle modalità del trattamento dettate dai principi di *privacy by design* e di *privacy by default*;
- alla valutazione dell'impatto sulla protezione dei dati personali (DPIA) se necessario.

Ogni Divisione/Direzione aziendale, nel caso di attivazione di un nuovo trattamento di dati personali e/o di modifica alle caratteristiche di un trattamento già esistente, dovrà provvedere a darne comunicazione all'Ufficio gestione dati personali – privacy mediante il modulo **M PRY 31** *Scheda rilevazione trattamento* da trasmette via mail.

L'Ufficio gestione dati personali – privacy provvederà al perfezionamento degli adempimenti sia provvedendovi direttamente sia fornendo assistenza nelle valutazioni legate all'eventuale DPIA e ai requisiti di *privacy by design* e di *privacy by default*.

10. Diritti dell'interessato

Ai sensi del GDPR l'interessato ha diritto di ottenere dalle società del Gruppo Veritas la conferma circa la conferma o meno di trattamenti di dati personali che lo riguardano.

Eventuali richieste di conferma circa l'esistenza o meno di trattamenti di dati personali, devono essere rivolte per iscritto dall'interessato utilizzando l'apposito modulo disponibile sui siti internet delle società del Gruppo Veritas e inoltrato, corredato da copia del documento di identità dell'interessato, all'indirizzo indicato sui

siti web delle società. La trasmissione può avvenire mediante lettera raccomandata, telefax o posta elettronica.

Eventuali richieste formulate oralmente devono comunque essere prese in carico e registrate dalle società del Gruppo Veritas a cura dell'incaricato o del responsabile-refente interessato a trattamento oggetto di indagine, e trattate come quelle giunte in azienda per iscritto.

In particolare, il GDPR garantisce all'interessato i seguenti diritti, che le società del Gruppo Veritas si obbligano ad assicurare:

- la conferma che siano o meno in corso attività di trattamento di suoi dati personali e informazioni sulle caratteristiche del trattamento (es. finalità, categorie di dati personali, destinatari della comunicazione dei dati, diritti dell'interessato);
- la rettifica di dati personali inesatti che lo riguardano, nonché la loro integrazione qualora siano incompleti;
- la cancellazione, se sussistono alcune fattispecie, ad esempio se i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, se l'interessato ha revocato il consenso o ha esercitato il diritto di opposizione al trattamento, oppure se i dati personali sono stati trattati illecitamente;
- la portabilità dei dati oggetto del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora il trattamento si basi su un consenso legittimo e sia effettuato con mezzi automatizzati;
- la cessazione del trattamento dei dati nel caso di trattamento effettuato sulla base del consenso dell'interessato.

Le procedure devono prevedere che, a seguito di ciascuna richiesta, si debbano fornire agli interessati le informazioni necessarie in forma concisa, accessibile ed usando un linguaggio semplice e chiaro, entro un mese (estendibile fino a due mesi, in casi di particolare complessità), anche in caso di diniego.

L'interessato, al fine di esercitare i diritti in materia di trattamento dati personali, può conferire delega o procura scritta a persone fisiche, enti, associazioni od organismi. In tal caso la persona che agisce per conto dell'interessato deve esibire e allegare alla richiesta copia della procura in oggetto, (ovvero di una delega sottoscritta in presenza di un incaricato aziendale o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato).

Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta deve invece essere avanzata da persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

I diritti di cui sopra, qualora concernenti persone decedute, possono essere esercitati dai legittimari ovvero dai soggetti che agiscano a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

11. Riferimenti normativi e documentali

riferimenti	
Regolamento UE 679/2016 GDPR	
dlgs 101/2018	
Sanzioni penali	
dlgs 196/2003	Così come novellato dal dlgs 101/2018
Provvedimenti Garante Privacy	
REG TEC	Regolamento per l'utilizzo del sistema informatico Gruppo Veritas
Guida aziendale	Privacy - Guida ad uso dei dipendenti
Registro delle attività di trattamento	
PR PRY 00	PR PRY 00 Valutazione e nomina responsabili esterni di trattamento dati personali ai sensi del Regolamento UE 679/2016 GDPR – Gruppo Veritas
PR PRY 01	PR PRY 01 Gestione degli incidenti informatici e degli incidenti agli archivi cartacei.
M PRY 29	Registro incidenti informatici (data breach)
M PRY 30	Comunicazione data breach al Garante Privacy
M PRY 31	Scheda rilevazione trattamento
M PRY	Informative trattamento dati personali (le informative sono tutte codificate M PRY)
M ECO 08	Modulo per il conferimento di materiale proveniente da piccoli lavori di manutenzione e ristrutturazione domestica
M ECO 09	