GDPR

General Data Protection Regulation

Redatto da
COMETA A.S.M.M.E.

RGPD

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

AD USO DEGLI INCARICATI

Revisione 00 – 18/07/2019

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato dall'Azienda COMETA A.S.M.M.E. (da questo punto in poi chiamata Azienda) con sede legale in Via Monte Sabotino 12/A 35020 Ponte San Nicolò PD, Codice Fiscale 92065090281 (nel seguito del documento indicata come Titolare del Trattamento).

Si precisa che, in qualità di Presidente del Consiglio di Amministrazione, firma come Titolare del Trattamento la Sig.ra Marzenta Anna Maria, nato a Piove di Sacco PD il 20/09/1958, residente in Via Garibaldi 3 PD, C.F.: MRZNMR58P60G693S.

Il presente documento e redatto e firmato in calce dal Titolare del trattamento (Data Controller).

INDICE

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

1. Alcuni riferimenti generali direttamente dai Regolamento Europeo n. 679/2016

1.1 Disposizioni generali

Articolo 1
Oggetto e finalità (C1-14, C170, C172)

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

2. Il presente regolamento protegge i diritti e le liberta fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. La libera circolazione dei dati personali nell'Unione non può essere limitata nè vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 2
Ambito di applicazione materiale (C 15-21)

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento non si applica ai trattamenti di dati personali:

   a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
   b) effettuati dagli Stati membri nel'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
   c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; (C18)
   d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alfa sicurezza pubblica e la prevenzione delle stesse.

3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.

4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Articolo 3
Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. (C22)

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuate da un titolare del trattamento o da un responsabile del trattamento che non e stabilito ell'Unione, quando le attività di trattamento riguardano: (C23, C24)

   a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
   b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto intenzionale pubblico. (C25)

Articolo 4
Definizioni

Ai fini del presente regolamento s'intende per:

1. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)

2. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3. «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

4. «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

5. «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conserva te separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

6. «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (C15)

7. «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

8. «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9. «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)

10. «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11. «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

12. «violazione dei dati personali»: 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; (C85)

13. «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)

14. «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)

15. «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35)

16. «stabilimento principale»: (C36, C37)
    a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
    b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17. «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

18. «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19. «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

20. «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

21. «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22. «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124)
    a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
    b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
    c) un reclamo è stato proposto a tale autorità di controllo;

23. «trattamento transfrontaliero»:
    a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
    b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24. «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25. «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
26. «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

1.2 Codice Penale

Articolo 392

Questo articolo tratta dell'esercizio arbitrario delle proprie regioni con violenza sulle cose. Appartiene al libro II, titolo III del codice penale che comprende i fatti criminosi che costituiscono ostacolo o turbamento al normale svolgimento dell'attività giudiziaria. II legislatore ha voluto punire tutti quei comportamenti che hanno come obiettivo l'alterazione, la modifica o la distruzione dei programmi. II riferimento all'esercizio delle proprie ragioni e significativo in quanto si ritiene che tali comportamenti non siano motivati da vandalismo ma dal desiderio di ostacolare o impedire il corretto svolgimento delle attività di un sistema come azione di rivalsa per eventuali danni o torti subiti. Affinché il reato sia configurabile devono sussistere due condizioni: l'esistenza di un preteso diritto e la tutelabilità di tale diritto mediante ricorso all'autorità giudiziaria.

Articolo 420
Attentato a impianti di pubblica utilità

Questo articolo modifica il precedente, aggiungendo alla fattispecie di impianti di pubblica utilità anche i sistemi informatici e telematici, includendo i dati, le informazioni e i programmi che ne fanno parte. II reato e trattato nel libro II, titolo V del codice penale che elenca tutti i fatti criminosi diretti a sovvertire l'ordine pubblico. II reato di attentato è definito tra quelli a consumazione anticipate, separando l'atto di preparazione da quello di esecuzione. La novità di questo articolo consiste nell'inclusione dei sistemi informatici e telematici tra quelli di pubblica utilità. Non si deve confondere la pubblica utilità con la pubblica amministrazione. Sono considerati impianti di pubblica utilità tutti quelli considerati essenziali per lo svolgimento ordinato e regolare della vita sociale.

Articolo 491 bis
Documenti informatici

Questo articolo costituisce una novità in quanto introduce esplicitamente il concetto di documento informatico, difendendolo dalle azioni volta a falsificarlo. L'articolo fa parte del libro II, titolo VII dedicato ai reati contro la fede pubblica. In particolare, il reato 6 contemplato tra quelli relativi alle falsità in atti. La portata dell'articolo 6 notevole per l'esplicito riconoscimento del valore dei documenti informatici, al pari di quello assicurato ai documenti cartacei. II legislatore ha voluto superare la tradizionale associazione documento, supporto di registrazione concentrando l'attenzione sul contenitore (e quindi sulle azioni volte a falsificarlo, genericamente indicate come falso materiale) e sul contenuto (e quindi sulle azioni volte a dichiarare il falso, genericamente indicate come falso ideologico). Prima di superare le difficoltà legate al riconoscimento della paternità dell'autore di un documento sarà necessario attendere l'emanazione di un'altra legge, quella che definisce la firma digitale.

Articolo 615 ter
Accesso abusivo a un sistema informatico o telematico

II titolo XII del libro II del codice penale è dedicato ai delitti contro la persona. In particolare, la sezione IV del capo III è dedicata ai delitti contro l'inviolabilità del domicilio. È in questo contesto che sono stati inquadrati i tre nuovi articoli introdotti dalla legge 547. II primo di essi punisce l'accesso all'interno di un sistema informatico, qualora questo accesso non si svolga secondo quanto legittimamente prescritto. Il concetto di domicilio è esteso al perimetro dei sistemi informatici, superando così tutte le difficoltà incontrate in precedenza net cast di accesso abusivo. La legge considera reato anche il solo accedere a un sistema informatico senza danneggiarlo, concetto recentemente rafforzato dalia legge sula tutela dei dati personali che difende tali dati da un uso non legittimo. L'articolo prevede che

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

il sistema sia protetto da misure di sicurezza ma non richiede che tali misure siano necessarie, essendo l'accesso abusivo se effettuato contro fa volontà dl chi ha il potere di escluderlo.

Articolo 615 quarter
Detenzione e diffusione abusiva di codici di accesso a un sistema informatico o telematico

Collegato al precedente, questo articolo sanziona che il possesso e fa detenzione abusiva dei codici di accesso. L'attenzione delta legge e rivolta al momento della raccolta dei codici, rendendo esplicitamente illegale l'attività di coloro che mettono in essere le tecniche di appropriazione indebita di password. I momenti successivi a questa attività, riproduzione, diffusione, comunicazione e consegna dei codici, sono sanzionati esplicitamente. La legge intende così definire con precisione tulle quelle situazioni in cui si mette a repentaglio la sicurezza dei sistemi informatici per evitare che tali comportamenti debbano essere puniti per analogia con altri comportamenti criminosi. II ricorso dell'analogia nel diritto penale è espressamente vietato dalla Costituzione.

Articolo 615 quinquies.
Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

Ultimo delta trilogia dedicata alla protezione del domicilio informatico, questo articolo individua con precisione tulle queste situazioni in cui un sistema informatico e danneggiato dall'interno. Il caso tipico è rappresentato dai cosiddetti virus che, nelle sembianze di programmi o di frammenti di codice eseguibile, danneggiano o interrompono il regolare funzionamento di un sistema informatico. Anche in questo caso il legislatore ha voluto definire con precisione una nuova fattispecie, non riconosciuta dalla giurisprudenza precedente all'entrata in vigore della legge 547.

Articolo 616

La corrispondenza, i suoi diritti e i reati relativi ad essa sono contenuti nel libro II del codice penale, at titolo XII, capo III (delitti contro la libertà individuale), sezione V (delitti contro l'inviolabilità dei segreti). La modifica apportata all'articolo introduce la modalità informatica e telematica tra quelle con cui è possibile inviare corrispondenza. Com'è noto, la corrispondenza è protetta dal segreto, a garanzia del diritto di opinione, l'uso della posta elettronica rappresenta solo un'alterativa alla posta ordinaria, che non perde così il suo diritto a essere protetta.

Articolo 617 quater
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Il problema dell'intercettazione è affrontato da tre articoli che entrano nel merito di questa fattispecie quando riguarda comunicazione effettuate mediante sistemi informatici o telematici. L'articolo in questione, inserito come il precedente tra i delitti contro l'inviolabilità dei segreti, sanziona tutti quei comportamenti criminosi volti a intercettare la comunicazione tra sistemi. È interessante notare il riferimento esplicito alla figura dell'operatore di sistema il quale non può abusare del suo polere tecnico, necessario per lo svolgimento efficace del suo compito, per intercettare le comunicazioni che avvengono all'interno dei sistemi da lui gestiti. Tale comportamento, comunemente ipotizzato come naturale e necessario in alcune situazioni, e invece identificato e sanzionato con precisione.

Articolo 617 quinquies
Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Sulla falsa riga del precedente, questo articolo identifica tutti quei comportamenti che hanno il fine di rendere possibile l'intercettazione di comunicazioni telematiche o informatiche.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Articolo 617 sexies
Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche

Ultimo della trilogia dedicata all'intercettazione di comunicazioni telematiche o informatiche, questo articolo sancisce l'inviolabilità delle comunicazioni informatiche o telematiche difendendole da atti che mirano a cambiarne il contenuto.

Articolo 621
II tema dell'inviolabilità dei segreti è affrontato in questo articolo, modificato dalla legge 547, in modo che il concetto di documento sia esteso a tutti quei supporti informatici che contengono dati, informazioni o programmi. In questo modo, anticipando l'emanazione di successivi dispositivi, il legislatore ha voluto dare ai documenti informatici lo stesso valore e la stessa salvaguardia assegnata ai documenti cartacei o di qualsiasi natura. In assenza di questa precisa disposizione, il supporto informatico era considerato valido ed equivalente a quello cartaceo solo quando il suo contenuto era rappresentato fisicamente e, pertanto, direttamente intellegibile da parte di una persona fisica.

Articolo 623 bis
Altre comunicazioni e conversazioni
La sostituzione operate da questo articolo elimina tutte le controversie sorte dalla dizione precedente in cui si affermava che le comunicazioni e le conversazioni dovessero avvenire con collegamento a filo o ad onde guidate. Nella nuova formulazione si aggiunge la modalità informatica e telematica e si elimina la restrizione tecnologica del mezzo di trasmissione. In questa nuova formulazione, la trasmissione a distanza di suoni, immagini o altri dati è protetta dalle disposizioni contenute nella sezione del codice penale.

Articolo 635 bis
Danneggiamento di sistemi informatici e telematici
L'articolo in questione fa parte del libro II del codice penale, nel titolo XIII (delitti contro il patrimonio), capo 1 (delitti contro il patrimonio mediante violenza alle cose o alle persone). Il bene tutelato è il sistema informatico o telematico, contro le azioni di danneggiamento. In caso di reato commesso da chi abusa della qualità di operatore di sistema si applicano le aggravanti. È da notare che la diffusione o la comunicazione di virus è sanzionata dall'articolo 615 quinquies. La comunicazione di virus mediante posta elettronica è, pertanto, un fatto criminoso che unisce alla diffusione del virus anche il danneggiamento causato dalla sua attivazione nel sistema bersaglio.

Articolo 640 ter
Frode Informatica
II reato di frode informatica, specificamente previsto nel libro II, titolo XIII (delitti contro il patrimonio), capo II (delitti contro il patrimonio mediante frode) estende il concetto di frode a tutti quei comportamenti in cui si induce in errore un sistema informatico o telematico. La norma e fortemente innovativa in quanto supera tutte le difficoltà insite nell'equiparazione di una sistema impersonale, oggetto dl truffa, a una persona fisica. Le modalità con cui la frode può essere condotta sono mono varie. Tra di esse le più comuni sono le azioni sui dati inseriti all'interno del sistema, le azioni sul programma, le azioni sulle informazioni prodotte dal sistema. In tutti questi casi il comportamento mira ad attivare un espediente che inganna o un'attività che falsa la realtà.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

1.3 Codice di procedura penale

Articolo 266 bis
Intercettazioni di comunicazioni informatiche e telematiche

Le modifiche operate sul codice penale hanno reso necessari alcuni aggiustamenti nel codice di procedura penale. L'articolo autorizza le intercettazioni di comunicazioni informatiche e telematiche per tutti i reati mediante l'uso di queste tecnologie, oltre che a quelli già previsti in precedenza.

Articolo 266
Articolo tecnico che modifica le modalità di esecuzione delle intercettazioni, alla luce delle modifiche operate dagli articoli precedenti.

Decreto legge 8 giugno 1992, n. 306
Articolo 25 ter
Articolo tecnico che raccorda il dettato dell'articolo 266 bis con quello dell'articolo 25 del decreto legge citato.

1.4 Altri riferimenti

Articolo 2087 del Codice Civile
L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori dl lavoro.

Articolo 2049 del Codice Civile
I padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti.

Articolo 2050 del Codice Civile
Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

Articolo 7 co. 1 legge 300/1970
Le norme disciplinari relative alle sanzioni, alle infrazioni in relazione alle quali ciascuna di esse può essere applicata ed alle procedure di contestazione delle stesse, devono essere portate a conoscenza dei lavoratori mediante affissione in luogo accessibile a tutti. Esse devono applicare quanto in materia è stabilito da accordi e contratti di lavoro ove esistano.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

2. Normativa di riferimento

- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
- ISO 27001 – Analisi dei rischi
- Comunicazioni del Garante della Privacy (www.garanteprivacy.it)
- Linee guida Garante Europeo recepite e tradotte dal Garante della Privacy (www.garanteprivacy.it)

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

3. Introduzione

La redazione del presente regolamento generate sulla protezione dei dati personali (da questo punto in poi GDPR) si attiene a quanto indicato net Regolamento Europeo n. 679 del 2016, segue le linee guida ed i chiarimenti fomiti dal Garante per la Privacy e disponibili sul sito del Garante stesso.

Il presente GDPR nello specifico prosegue:

a) descrivendo i Fondamenti di liceità del trattamento;
b) predisponendo un'adeguata informativa per tutti gli interessati;
c) indicando i diritti degli Interessati;
d) predisponendo il/i registro/i delle attività di trattamento dei dati personali;
e) procedendo alla distribuzione dei compiti e delle responsabilità (individuazione delle figure principali quali il Titolare, responsabile, incaricato, ecc.);
f) analizzando i rischi derivanti dai trattamenti;
g) indicando le misure di accountabilty decise dal Titolare e/o Responsabile del trattamento;
h) verificando l'eventuale presenza di trasferimenti intenzionali di dati personali.
i) indicando le misure, già adottate e da adottare, per garantire l'integrità e la disponibilità dei dati;
j) indicando i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento;
k) dettando i criteri da adottare, per garantire l'adozione delle misure minime di scurezza, in caso di trattamenti di dati personali affidati all'esterno;
l) indicando le procedure da seguire per il controllo sullo stato della sicurezza;
m) dichiarazioni d'impegno e firma.

A titolo di chiarimento e trasparenza di seguito diamo maggiori informazioni in relazione ad alcuni dei punti sopra indicati.

3.1 Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'articolo 6 del regolamento (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

3.1.1 Il consenso

In particolare:

- per i dati particolari cosiddetti "sensibili" (si veda l'articolo 9 regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa fa profilazione - articolo 22);

- non deve essere necessariamente "documentato per iscritto", ne e richiesta fa "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (articolo 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;

- il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle pre-spuntate);

- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

3.2 Informativa

3.2.1 Contenuti dell'informativa

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento. In particolare, il titolare deve sempre specificare i dati di contatto del RPD - DPO (Responsabile della protezione dei dati – Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.
Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.
Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

3.2.2 Tempi dell'informativa

L'informativa (disciplinata nello specifico dagli articoli 3 e 4 del regolamento) deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato - articolo 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (articolo 4 del regolamento), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità, e quali sono i destinatari del dati.

NOTA: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Nel caso di dati personali non raccolti direttamente presso l'interessato (articolo 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure ai momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato).

3.2.3 Modalità dell'informativa

Il regolamento specifica le caratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano articolo 2, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (articolo 2, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

forma sintetica, ma solo "in combinazione" con l'informativa estesa (articolo 2, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.
Sono inoltre parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa (si veda articolo 3, paragrafo 4 e articolo 4, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare, in caso di dati personali raccolti da fonti diverse dall'interessato, valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato (si veda articolo 4, paragrafo 5, lettera b).

3.3 Diritti degli interessati

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare dove comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (articolo 12.5), ovvero se sono chiesto più "copie" dei dati personali nel caso del diritto di accesso (articolo 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola dove avvenire in forma scritta anche attraverso strumenti elettronica che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (articolo 2, paragrafo 1, si veda anche articolo 15, paragrafo 3).
La risposta fornita all'interessato non dove essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

3.3.1 Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli articoli 11 e 12 del regolamento.
Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. Benché sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti (articoli 5-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (articolo 28, paragrafo 3, lettera e).
L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi eccezioni (si veda sopra).
Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, articolo 11, paragrafo 2 e articolo 12, paragrafo 6).
Sono ammesse deroghe ai diritti riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, articoli 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", articolo 83 *trattamenti di natura giornalistica* e articolo 89 *trattamenti per finalità di ricerca scientifica o storica o di statistica*).
In questo senso, in via generale, possono continuare a essere applicate tutte le deroghe previste dall'articolo 8, comma 2, del Codice relativo al D.Lgs. n. 196/2003 in quanto compatibili con le disposizioni citate. Al riguardo, il Garante sta valutando la piena rispondenza delle disposizioni citate in tale articolo del Codice con i requisiti fissati per la legislazione nazionale dall'articolo 23, paragrafo 2, del regolamento.

3.4 Titolare, Responsabile, Incaricato del trattamento

Il regolamento:

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- disciplina la contitolarità del trattamento (articolo 26) e impone ai titolari 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;

- fissa dettagliatamente 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'articolo 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, le 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;

- consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda articolo 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 dei risarcimento di eventuali danni causati dai trattamento, salvo dimostri che l'evento dannoso" non gli è in alcun modo imputabile" (si veda articolo 82, paragrafo 1 e paragrafo 3);

- prevede 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 articolo 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex articolo 32 regolamento); la designazione di un RPD - DPO (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati recentemente pubblicate dal Gruppo "Articolo 29" dopo essere state sottoposte a consultazione pubblica, disponibili qui anche nella versione in italiano: www.garanteprivacy.it/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda articolo 37 del regolamento). Si ricorda, inoltre, Che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'articolo 27, paragrafo 3, del regolamento, diversamente da quanto prevede oggi l'articolo 5, comma 2, del Codice.

Il regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). Pur non prevedendo espressamente la figura dell'"incaricato" del trattamento (ex articolo 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, articolo 4, n. 10, del regolamento).

3.5 Approccio basato sul rischio e misure di accountability (responsabilizzazione) di titolari e responsabili

Il regolamento pone con forza facendo Sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concrete adozione di misure analizzate ad assicurare l'applicazione del regolamento (si vedano articoli 23-25, in particolare, e l'intero Capo IV del regolamento). 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 e sintetizzato dall'espressione inglese "data protection by default and by design" (si veda articolo 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 liberta 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'articolo 25(1) del regolamento) e

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

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 liberta e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano articoli 35-36) 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 (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati recentemente pubblicate dal Gruppo "Articolo 29" dopo essere state sottoposte a consultazione pubblica, disponibili qui anche nella versione in italiano: www.garanteprivacy.it/DPIA). 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'articolo 58: 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 si collocherà successivamente 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 italiano, come la notifica preventive dei trattamenti all'autorità di controllo e il cosiddetto *prior checking*, 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. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fomite ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Nei paragrafi seguenti si richiamano alcune delle principali novità in termini di adempimenti da parte di titolari e responsabili del trattamento.

3.5.1 Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda articolo 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'Azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. il registro deve avere forma scritta, anche elettronica, e dove essere esibito su richiesta al Garante.

Raccomandazioni
La tenuta del registro dei trattamenti non costituisce un adempimento formate 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. I contenuti del registro sono fissati, come detto, nell'articolo 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportune proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

3.5.2 Misure di sicurezza

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (articolo 32, paragrafo 1); in questo senso, la lista di cui al paragrafo 1 dell'articolo 32 è una lista aperta e non esaustiva ("tra le altre, se del caso"). Per lo stesso motivo, non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex articolo 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da articolo 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guide o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'articolo 6, paragrafo 1, lettere c ed e del regolamento) potranno restare in vigore (in base all'articolo 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di elevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex articoli 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

3.5.3 Notifica delle violazioni di dati personali

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazioni derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34. I contenuti della notifica all'autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli articoli 33 e 34 del regolamento. Su questo e su tutta la disciplina in materia, il Comitato europeo della protezione dati (si veda articolo 70, paragrafo 1, lettere g e h) è chiamato a formulare linee guida specifiche, alle quali sta già lavorando il Gruppo "Articolo 29".

Raccomandazioni
Tutti i titolari di trattamenti dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda articolo 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'articolo 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

3.5.4 Responsabile delta protezione dei dati (RPO) - Data Protection Officer (DPO)

Anche la designazione di un "responsabile della protezione dati" (RPO, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante Che e proprio del regolamento (si veda articolo 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare o del responsabile. Non e un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'articolo 35. La sua designazione è obbligatoria in alcuni casi (si veda articolo 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive dl questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano articoli 36 e 39) in termini che il WP29 ha

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante.

3.6 Trasferimenti di dati verso paesi terzi e organismi internazionali

In primo luogo, viene meno il requisito dett'autorizzazione nazionale (si vedano articolo 45, paragrafo 1, e articolo 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'articolo 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante, a differenza di quanto attualmente previsto dall'articolo 44 del Codice.
Tuttavia, l'autorizzazione del Garante sarà ancora necessaria se un titolare desidera utilizzare clausole contrattuali ad-hoc (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure accordi amministrativi stipulati tra autorità pubbliche, una delle novità introdotte dal regolamento.
Il regolamento consente di ricorrere anche a codici di condotta ovvero a schemi di certificazione per dimostrare le "garanzie adeguate" previste dall'articolo 46. Ciò significa che i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. Tuttavia (si vedano articolo 40, paragrafo 3, e articolo 42, paragrafo 2), tali titolari dovranno assumere, inoltre, un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento che sia giuridicamente vincolante e azionabile dagli interessati.
Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative ammesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda articolo 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui l'articolo 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un interesse pubblico riconosciuto dal diritto dello Stato membro del titolare o dal diritto del'Ue (si veda articolo 49, paragrafo 4),e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.
Il regolamento fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme. L'elenco indicato al riguardo nel paragrafo 2 dell'articolo 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esaustivamente attraverso il meccanismo della coerenza di cui agli aricoli 63-65 del regolamento, ossia, è previsto in ogni caso l'intervento dal Comitato europeo per la protezione dai dati (si veda articolo 65, paragrafo 1, lettera d).
Il regolamento (si veda Capo V) ha confermato l'approccio attualmente vigente in base alla direttiva 95/46 e al Codice italiano per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

1) adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea (si veda articolo 44, comma 1, lettera b, del Codice);

2) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa, BCR e clausole contrattuali modello) (si veda articolo 44, comma 1, lettera a del Codice);

3) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni (corrispondenti in parte alle disposizioni del'articolo 43, comma 1, del Codice).

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Le decisioni di adeguatezza finora adottate dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifiche (si veda articolo 45, paragrafo 9 e articolo 96). Restano valide, conseguentemente, le autorizzazioni nazionali finora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione. Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda aricolo 46, paragrafo 5), sino a loro eventuale modifica.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

4. Descrizione dell'attività dell'azienda ed informazioni generali preliminari

L'Azienda COMETA A.S.M.M.E. opera nell'ambito socio-assistenziale e nella tutela e promozione dei diritti dei malati di malattie metaboliche ereditarie e delle loro famiglie.

4.1 Caratteristiche di aree, locali e strumenti con cui si effettuano i trattamenti

- ✓ La sede di COMETA A.S.M.M.E. si trova in un edificio (E1) costituito da un piano fuori terra, situato in Via Monte Sabotino 12/A 35020 Ponte San Nicolò PD
- ✓ Tutte le funzioni di trattamento sono svolte all'interno dell'edificio (E1).
- ✓ L'edificio ha un accesso principale normalmente controllato durante l'orario di lavoro dal personale della Segreteria/reception.
- ✓ L'accesso all'edificio da parte del personale è autorizzato mediante riconoscimento a vista.
- ✓ Per gli esterni all'Azienda è richiesta la qualificazione e il riconoscimento
- ✓ Tutti i locali sono climatizzati.
- ✓ Negli ambiti di lavoro di ogni funzione aziendale si possono trovare due tipi di archivi ACI e AC2:
  L'archivio AC1 raccoglie la documentazione di natura sia amministrativa, sia tecnica attualmente utilizzata per i rapporti di lavoro in corse dalle funzioni dell'ambito al quale appartiene l'archivio.
  L'archivio AC2 raccoglie prevalentemente la documentazione storica di natura sia amministrativa, sia tecnica. Ha praticamente dati di tutte le funzioni aziendali.
- ✓ Tutti gli apparati attivi relativi alla rete aziendale e tutte le apparecchiature di telefonia sono ospitate in appositi spazi controllati. Tali zone sono presidiate costantemente e non sono accessibili dagli esterni all'Azienda.
- ✓ Gli archivi sono normalmente chiusi, e le chiavi sono custodite da un numero ristretto di persone autorizzate (membri della Direzione-Amministrazione).
- ✓ Le persone esterne possono accedere a tali archivi solamente dopo essere stati autorizzati ed in maniera controllata (registro d'ingresso e di uscita).
- ✓ Dopo l'orario di lavoro anche le persone interne possono accedere agli archivi solamente con autorizzazione ed in maniera controllata (registro d'ingresso e di uscita).
- ✓ Per il trattamento dei dati su supporto cartaceo vengono utilizzati armadi, classificatori e cassetti, protetti da chiave.
- ✓ L'intera area è protetta da un sistema d'allarme con combinatore telefonico. L'intera area è soggetta al controllo di un istituto di vigilanza.

4.2 Sistema informatico

Per il trattamento informatico dei dati il Titolare si avvale di un sistema basato su rete locale (vedere allegato 5 per conoscere la composizione della struttura informatica e vari apparti utiizzati dal Titolare del Trattamento) formato da due computer e da un nas.
Si precisa che la gestione e controllo della struttura di rete viene effettuata periodicamente dall'amministratore di sistema (vedi paragrafo a seguire).

4.3 Descrizione delle varie postazioni (Client) utilizzate dalle varie funzioni

La postazione è stata associata agli incaricati al trattamento mediante le lettere d'incarico preparate par ognuno di questi e allegate al presente documento nelle quali sono anche segnalate le banche dati che tali incaricati sono autorizzati ad utilizzare (alle quali hanno accesso).

- ✓ La rete è costituita da una sezione a 10/100/1000 Mbit/s alla quale si collega la postazione aziendale.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- ✓ Alla sezione a 10/100/1000 Mbit/s sono collegate varie apparecchiature (vedere allegato 5) configurate per gestire il collegamento della LAN.
- ✓ La navigazione e la gestione della posta elettronica avvengono tramite un ponte radio e una linea ADSL. L'intero sistema è protetto da antivirus.
- ✓ I dati sono backuppati giornalmente tramite un NAS Q-Nap.
- ✓ Un backup viene fatto ciclicamente poi anche su un hard disk esterno. Il tutto viene tenuto in un luogo sicuro.
- ✓ Tutti i client possono navigare (in modalità controllata) in Internet e possono gestire la posta elettronica (vedere manuale per la sicurezza).
- ✓ L'accesso alle stazioni e ai dati è gestito mediante la validazione degli Utenti ed utilizza gli strumenti standard offerti dal sistema operativo.
- ✓ Agli Utenti è demandato il compito di spostare nelle cartelle personali i documenti e i dati che desiderano vengano salvati periodicamente.
- ✓ Tutti i Client utilizzano un antivirus software con aggiogamento in automatico.
- ✓ In virtù di quanto indicato e delle caratteristiche dei sistemi operativi installati sui Client, risultano implementati i seguenti livelli di protezione sicurezza:
  - Le applicazioni della società sono dotate di credenziali di autenticazione univoche rispettanti i parametri richiesti dalla norma.
  - L'accesso ai dati personali avviene sempre tramite account assegnati personalmente agli incaricati autorizzati.
  - Le password prevedono regole di complessità e una scadenza.
  - Il sistema antivirus è costantemente aggiornato.
  - Eventuali telefoni smarthphone, tablet e notebook se utilizzati estremamente all'azienda sono normalmente protetti da software di cifratura.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

A. Fondamenti di liceità del trattamento
B. Informative
C. Diritti degli interessati

Vedere le informative predisposte e allegate al presente documento.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

D. Il registro delle attività di trattamento di dati personali

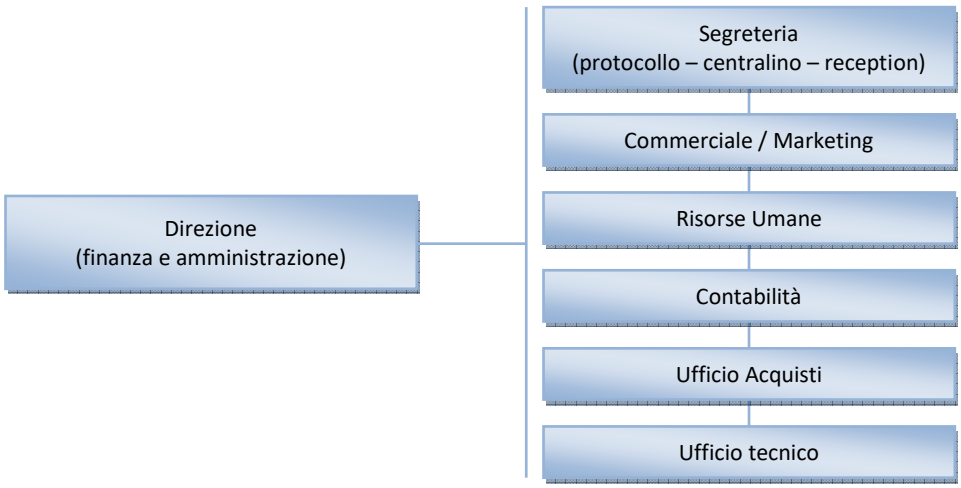
Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda articolo 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'articolo 30. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'Azienda o di un soggetto pubblico indispensabile per ogni valutazione e analisi del rischio.
Seguendo le raccomandazioni del Garante Il quale precisa che la tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali, il Titolare del trattamento ha deciso di predisporre tale registro così da poter effettuare un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche e successivamente un'attenta analisi dei rischi. I contenuti del registro seguente seguono quanto fissato nell'articolo 30 del Regolamento.

D.1 L'elenco dei trattamenti dei dati personali

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare, si procede come segue:
si individuano i tipi di dati personali trattati in base alla loro natura (comuni, giudiziari o sensibili, ecc.) ed alla categoria di soggetti cui essi si riferiscono (clienti, fornitori, utenti, personale, collaboratori, ecc.).

D.2 Tipologie dei dati trattati

Non essendo passibile una catalogazione puntuale delle singole banche dati per la varietà e continua mutazione della stesse a parità di trattamento, la rilevazione dei trattamenti dei dati, posti in essere dal Titolare, viene effettuata analizzando le tipologie di dati trattate da ciascuna Funzione dell'Azienda.
A ogni tipologia vengono associati un codice (Txx) ed una denominazione.
Il seguente diagramma rappresenta in forma semplificata le Funzioni operanti nell'ambito dell'Azienda.



Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

IN ALLEGATO AL PRESENTE DOCUMENTO

Allegato 1
Gli ambiti delle varie funzioni individuate

Ponte San Nicolò

Firma Autore dell'individuazione degli ambiti
Marzenta Anna Maria

_____

Allegato 2
II registro delle attività di trattamento e delle misure tecniche e organizzative di sicurezza redatto dal titolare del trattamento

Ponte San Nicolò

Firma Autore delle attività di trattamento
Marzenta Anna Maria

_____

Allegato 3
L'analisi dei rischi

Ponte San Nicolò

Firma Autore delle attività di trattamento
Marzenta Anna Maria

_____

Allegato 4
Il piano di trattamento dei rischi

Ponte San Nicolò

Firma Autore delle attività di trattamento
Marzenta Anna Maria

_____

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

D.3 Riepilogo dei trattamenti di dati personali precedentemente indicati nel registro di trattamenti

Le seguenti tabelle riassumono e completano quanto descritto nelle pagine precedenti (allegato 2).

Tabella 1. Elenco di informazioni essenziali dei trattamenti di dati personali

Codice	Finalità perseguita o attività svolta	Categorie di interessati	Art. 9	Art. 10	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
T1	Adempimenti contabili	Clienti	X	X	Direzione	Commerciale / marketing Contabilità Ufficio Tecnico Studio Commercialista Studio Paghe	Archivi cartacei PC in LAN
T2	Adempimenti contabili	Fornitori			Direzione	Contabilità Commerciale/ Marketing Segreteria Acquisti Ufficio Tecnico Studio Commercialista	Archivi cartacei PC in LAN
T3	Adempimenti contabili	Altri soggetti			Direzione	Contabilità Studio Commercialista	Archivi cartacei PC in LAN
T4	Adempimenti contabili	Titolare			Direzione	Contabilità Studio Commercialista	Archivi cartacei PC in LAN
T5	Adempimenti amministrativi	Soci amministratori			Direzione	Contabilità Studio Commercialista	Archivi cartacei PC in LAN
T6	Gestione contenziosi	Altri soggetti		X	Direzione		Archivi cartacei PC in LAN
T7	Adempimenti contabili / accordi	Fornitori			Direzione	Contabilità	Archivi cartacei PC in LAN
T8	Gestione personale	Personale / collaboratori			Risorse Umane	Contabilità	Archivi cartacei PC in LAN
T9	Gestione personale	Personale / collaboratori	X		Risorse Umane	Contabilità	Archivi cartacei PC in LAN
T10	Gestione personale	Personale / collaboratori	X		Risorse Umane		Archivi cartacei PC in LAN
T11	Gestione personale	Personale / collaboratori	X		Risorse Umane		Archivi cartacei PC in LAN
T12	Gestione personale	Personale / collaboratori	X		Risorse Umane		Archivi cartacei PC in LAN
T13	Gestione personale	Personale / collaboratori			Risorse Umane		Archivi cartacei PC in LAN
T14	Gestione tecnica / attività commerciale	Clienti / possibili clienti			Tecnico / Commerciale		Archivi cartacei PC in LAN

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Codice	Finalità perseguita o attività svolta	Categorie di interessati	Art. 9	Art. 10	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
T15	Gestione tecnica / attività commerciale	Clienti / possibili clienti			Tecnico / Commerciale		Archivi cartacei PC in LAN
T16	Gestione tecnica / attività commerciale	Clienti / possibili clienti			Tecnico / Commerciale	Contabilità	Archivi cartacei PC in LAN
T17	Gestione tecnica / attività commerciale	Clienti / possibili clienti			Tecnico / Commerciale	Contabilità Ufficio Tecnico	Archivi cartacei PC in LAN
T18	Gestione tecnica / attività commerciale	Clienti			Tecnico / Commerciale	Contabilità	Archivi cartacei PC in LAN
T19	Gestione tecnica / attività commerciale	Clienti			Tecnico / Commerciale	Contabilità Acquisti	Archivi cartacei PC in LAN
T20	Protocollo	Clienti / fornitori / altri soggetti			Segreteria	Direzione Contabilità	Archivi cartacei PC in LAN
T21	Gestione approvvigionamenti	Fornitori			Ufficio Acquisti	Contabilità	Archivi cartacei PC in LAN
T22	Redazione progetti	Clienti / servizi esterni			Ufficio Acquisti	Contabilità	Archivi cartacei PC in LAN

Per la distribuzione dei compiti e delle responsabilità si veda più avanti nel documenti

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Tabella 2. Elenco di ulteriori elementi per descrivere gli strumenti dei trattamenti di dati personali

Codice	Banca dati	Ubicazione fisica dei supporti di memorizzazione	Tipologia di dispositivi di accesso	Tipologia di interconnesione
T1	Clienti	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T2	Fornitori	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T3	Altri soggetti	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T4	Dati contabili	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T5	Dati amministratori	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T6	Contenziosi	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T7	Accordi particolari fornitori	Direzione Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T8	Personale / collaboratori	Risorse Umane	Archivio cartaceo PC	LAN
T9	Personale / collaboratori	Risorse Umane	Archivio cartaceo PC	LAN
T10	Personale / collaboratori	Risorse Umane	Archivio cartaceo PC	LAN
T11	Candidati	Risorse Umane	Archivio cartaceo	LAN
T12	Visite mediche	Risorse Umane	Archivio cartaceo	LAN
T13	Idoneità	Risorse Umane	Archivio cartaceo	LAN
T14	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T15	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T16	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T17	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T18	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T19	Clienti / possibili clienti	Commerciale Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T20	Protocollo	Segreteria Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T21	Ufficio acquisti	Ufficio Acquisti Archivio (AC1, AC2)	Archivio cartaceo PC	LAN
T22	Ufficio tecnico	Ufficio Tecnico Archivio (AC1, AC2)	Archivio cartaceo PC	LAN

Le banche dati sopra indicate si riferiscono alle tipologie di dati identificate (alle varie Funzioni individuate).
Nelle varie postazioni la gestione dei dati può essere fatta mediante catalogazione in cartelle (directory) venti nomi diversi (nomi più significativi per gli utenti) rispetto ai nomi delle funzioni delle quali contengono i dati.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Ovviamente sono previste nei vari client anche cartelle di uso comune a tutte le funzioni (cartelle di scambio) e cartelle di utilità.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

E. Mansionario privacy: la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Il Titolare del trattamento ha deciso di assumere gli incarichi di ordine organizzativo e direttivo, come segue:

- ✓ ha nominato un amministratore del sistema informativo (vedere lettera d'incarico) al quale ha conferito il compito di sovrintendere alle risorse del sistema informativo e di consentirne l'utilizzazione;
- ✓ ha nominato un responsabile del trattamento
- ✓ lo stesso responsabile del trattamento risulta essere soggetto incaricato autorizzato alla custodia delle credenziali incaricati al trattamento: il trattamento dei dati personali viene effettuato solo da soggetti che hanno ricevuto un formate incarico, mediante designazione per iscritto di ogni singolo incaricato, con la quale si individua puntualmente l'ambito del trattamento consentito.

Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- ✓ procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto e previsto per i dati di natura comune;
- ✓ modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;
- ✓ modalità per elaborare e custodire le password necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- ✓ prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici mentre è in corso una sessione di lavoro;
- ✓ procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- ✓ procedure per il salvataggio dei dati;
- ✓ modalità di custodia ed utilizzo dei supporti rimuovibili contenenti dati personali;
- ✓ dovere di aggiornarsi, utilizzando il materiale e gli strumenti fomiti dal Titolare, sulle misure di sicurezza.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo (tecnici, ecc.), siano essi interni o esterni all'organizzazione del Titolare, viene prescritto di non effettuare alcun trattamento sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.
Le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato in base alla unita organizzativa cui i soggetti appartengono: in tale modo il Titolare dispone di un quadro chiaro di chi fa cosa (mansionario privacy), nell'ambito del trattamento dei dati personali.
Periodicamente, si procede ad aggiornare la definizione dei dati cui gli incaricati sono autorizzati ad accedere e dei trattamenti che sono autorizzati a porre in essere (ambiti dei trattamenti), al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.
La stessa operazione viene compiuta per le autorizzazioni rilasciate ai soggetti incaricati della gestione o manutenzione degli strumenti elettronici.

Nella seguente tabella si riassumono i tratti salienti dell'attuale mansionario privacy, come segue:

- nella prima colonna sono indicate le Strutture cui appartengono i Soggetti Incaricati
- nella seconda colonna sono riportati i trattamenti effettuati da ciascuna Struttura
- la terza colonna espone la descrizione dei compiti e delle responsabilità della Struttura

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Tabella 3. Distribuzione dei compiti e delle responsabilità

Struttura incaricata	Trattamenti effettuati dalla Struttura	Descrizione dei compiti e delle responsabilità della struttura
Direzione	T1 Dati comuni relativi a clienti T2 Dati comuni relativi a fornitori T3 Dati comuni relativi ad altri soggetti T4 Dati di natura economico-finanziaria relativi al/i Titolare/i T5 Dati personali relativi ai Soci, agli amministratori T6 Dati relativi ai contenziosi T7 Dati relativi ai contratti con i fornitori	Direzione e Coordinamento Espletamento adempimenti amministrativi Gestione contabile e finanziaria
Risorse Umane	T8 Dati comuni relativi ai dipendenti T9 Dati amministrativi relativi ai dipendenti T10 Dati relativi alla carriera professionale dei dipendenti, di natura anche sensibile T11 Dati relativi ai candidati all'assunzione di natura anche sensibile T12 Dati di natura sensibile relativi alla salute del personale T13 Dati relativi all'idoneità dei dipendenti	Gestione del personale Controllo della gestione giuridica ed economica del personale (dipendenti/collaboratori)
Studio Commercialista	T1 Dati comuni relativi a clienti T2 Dati comuni relativi a fornitori T3 Dati comuni relativi ad altri soggetti T4 Dati di natura economico-finanziaria relativi al/i Titolare/i T5 Dati personali relativi ai Soci, agli amministratori	Direzione e coordinamento Espletamento adempimenti amministrativi Gestione contabile e finanziaria
Commerciale / Marketing	T14 Dati relativi a possibili clienti T15 Dati relativi a possibili fornitori / collaboratori /professionisti T16 Dati relativi alle offerte T17 Dati relativi ai contratti T18 Documentazione prevista per legge e/o richiesta dai vari enti T19 Documenti relativi alle commesse	Gestione offerte Gestione clienti, fornitori Gestione certificazioni Gestione documentazione prevista dalla Legge, Organi o Enti.
Segreteria	T20 Archivio protocollo	Gestione corrispondenza aziendale e piccoli approvvigionamenti
Contabilità	T1 Dati comuni relativi a clienti T2 Dati comuni relativi a fornitori T3 Dati comuni relativi ad altri soggetti T4 Dati di natura economico-finanziaria relativi al/i Titolare/i T5 Dati personali relativi ai Soci, agli amministratori T6 Dati relativi ai contenziosi T7 Dati relativi ai contratti con i fornitori T8 Dati comuni relativi ai dipendenti T9 Dati amministrativi relativi ai dipendenti T16 Dati relativi alle offerte T17 Dati relativi ai contratti T18 Documentazione prevista per legge e/o richiesta dai vari enti T19 Documenti relativi alle commesse T20 Archivio protocollo	Gestione contabilità Gestione rapporti con clienti e con Enti

Per conoscere le mansioni di ogni singolo incaricato è sufficiente leggere la lettera d'incarico a questo relativa (vedere le lettere d'incarico allegate al presente documento).
Nelle lettere d'incarico il Titolare del Trattamento indica la tipologia di dati che l'incaricato è autorizzato a trattare (Funzioni).

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

F. Analisi dei rischi che incombono sui dati

La stima del rischio complessivo, che grava su un determinato trattamento di dati, è il risultato della combinazione di due tipi di rischi:

- ✓ quelli insiti nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- ✓ quelli conseguenti al verificarsi di eventi potenzialmente dannosi per la sicurezza dei dati.

Si stima il grado di rischio, che dipende dalla tipologia dei dati trattati dal Titolare, combinando il fattore della loro appetibilità per i terzi con quello che esprime la loro pericolosità per la privacy del soggetto cui i dati si riferiscono.
Si nota che un grado di rischio alto, o addirittura elevatissimo, è collegato al trattamento dei seguenti dati, alla tutela dei quali devono quindi essere dedicate particolari attenzioni:

- ✓ quelli idonei a rivelare informazioni di carattere sensibile con un elevato grado di pericolosità per la privacy dei soggetti interessati;
- ✓ quelli che costituiscono un'importante risorsa per il Titolare, in relazione ai danni che conseguirebbero da una eventuale perdita, o trafugamento, dei dati.

Il rischio può inoltre essere valutato in base agli eventi potenzialmente dannosi per la sicurezza dei dati.
Alcuni degli eventi presi in considerazione sono di seguito indicati (si veda più avanti l'analisi dei rischi per vedere la lista completa dei rischi analizzati).

F.1 Comportamenti degli operatori

- ✓ sottrazione di credenziali di autenticazione;
- ✓ carenza di consapevolezza, disattenzione o incuria;
- ✓ comportamenti sleali o fraudolenti;
- ✓ errore materiale.

F.2 Eventi relativi agli strumenti

- ✓ Azione di virus informatici o di programmi suscettibili di recare danno.
- ✓ Spamming o tecniche di sabotaggio.
- ✓ Malfunzionamento, indisponibilità o degrado degli strumenti.
- ✓ Accessi esterni non autorizzati.
- ✓ Intercettazione di informazioni in rete.

F.3 Eventi relativi al contesto

- ✓ Accessi non autorizzati a locali/reparti ad accesso ristretto.
- ✓ Sottrazione di strumenti contenenti dati.
- ✓ Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.).
- ✓ Eventi distruttivi, dolosi accidentali o dovuti a incuria.
- ✓ Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).
- ✓ Errori umani nella gestione della sicurezza fisica.

F.4 Analisi del rischio completa

Vedere allegato 3.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

G. Piano del trattamento dei rischi (approccio basato sul rischio e misure di accountability)

Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari, ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concrete adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano articoli 23-25, in particolare, e l'intero Capo IV del regolamento). 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 e sintetizzate dall'espressione inglese "data protection by default and by design" (si veda articolo 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 precedere al trattamento dei dati vero e proprie ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'articolo 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicative 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 individuate 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 (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano articoli 35-36) 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.

Seguendo le indicazioni del Garante, il Titolare del trattamento dopo aver redatto il Registro dei trattamenti e aver fatto l'analisi dei rischi, ha predisposto un PIANO DI TRATTAMENTO DEI RISCHI (vedere allegato 4 al presente documento)

G.1 Notifica delle violazioni di dati personali

A partire dal 25 maggio 2018, tutti i titolari dovranno notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si Veda considerando 85). Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare del trattamento.

A tale riguardo il Titolare del trattamento dell'Azienda scrivente ha predisposto un apposito registro, allegato al presente, dove annoterà tutti i "Data Breach" accaduti e s'impegna a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.
Inoltre se la probabilità che i rischi per i diritti e le libertà degli interessati sarà elevata, informerà delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo".

G.2 Considerazioni finali

Per quanto riguarda i rischi presi in considerazione, vista la formazione effettuata agli incaricati mediante formazione diretta e fornitura di un manuale sulla sicurezza; considerato il controllo continuo che viene fatto sui sistemi informatici (hardware e software) ed il sistema di procedure approntato per contrastare l'azione di software dannosi o mal funzionanti; valutata la situazione oggettiva dei meccanismi di sicurezza esistenti presso la sede dell'Azienda e la

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

posizione fisica dei locali nonché l'ottemperanza a quanto richiesto dall'attuale legislazione esistente in materia di prevenzione incendi, inclusa la verifica periodica di caldaie, impianto elettrico, impianto di riciclo aria e condizionamento, si ritiene che i rischi considerati siano tutti contrastati e che la probabilità del loro verificarsi sia bassa e dipendente da eventi del tutto eccezionali.
Per quanto riguarda il rischio di perdita dei dati dovuta ad allagamento bisogna precisare che, vista la posizione dell'edificio (E1) si esclude che, salvo eventi imprevedibili e del tutto eccezionali, detto rischio possa verificarsi.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

H. TRASFERIMENTI INTERNAZIONALI DI DATI PERSONALI

Si precisa che l'Azienda non effettua alcun trattamento di dati personali che preveda il trasferimento internazionale di dati personali.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

I. Misure atte a garantire l'integrità e la disponibilità dei 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)

Nel presente paragrafo vengono descritte le misure adottate dal Titolare atte a garantire:

- la protezione delle aree e dei locali, nei quali si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- la sicurezza logica, nell'ambito dell'utilizza degli strumenti elettronici.

I.1 La protezione di aree e locali

Per quanto concerne il rischio d'area, legato a eventi di carattere distruttivo, gli edifici e i locali nei quali si svolge il trattamento sono protetti da:

- dispositivi antincendio (estintore);
- gruppo di continuità dell'alimentazione elettrica (per i computers)
- impianto di condizionamento.

Per quanta riguarda le misure atte ad impedire gli accessi non autorizzati, gli edifici e i locali nei quali si svolge il trattamento sono protetti da:

- l'accesso agli ambienti è controllato a vista dal personale della segreteria;

Gli impianti e i sistemi di cui è dotata l'Azienda:
- appaiono soddisfacenti, al fine di garantire le opportune misure di sicurezza, al trattamento di dati personali da essa svolti.
  Per l'anno 2019 sona quindi previsti semplicemente interventi di manutenzione.
- Nel medio periodo è previsto l'adeguamento/miglioramento tecnologico a base di Norma.

I.2 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, dischetti, pen-usb, ecc.), si e provveduto a istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.
Agli incaricati vengono date disposizioni, per iscritto, di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, è stato loro prescritto di rivolgersi ad un superiore, o direttamente al Titolare.
Di conseguenza, agli incaricati è prescritta di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.
Gli incaricati devono custodire in modo appropriato gli atti, i documenti e i supporti contenenti dati personali loro affidati per la svolgimento delle mansioni lavorative.
Cautele particolari sono previste per gli atti, documenti e supporti contenenti dati particolari (sensibili, giuridici, ecc.): agli incaricati viene in questo caso prescritta di provvedere al controllo e alla custodia in moda tale che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli incaricati sono stati dotati di:

- cassetti can serratura;

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- armadi chiudibili a chiave;

nei quali devono riporre i documenti contenti dati particolari (cosiddetti ex sensibili, ex giuridici, ecc.) prima di assentarsi dal posta di lavoro anche temporaneamente.
In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro qualora l'incaricato debba continuare a utilizzarli nei giorni successivi.
Al termine del trattamento l'incaricato dovrà invece riporre nell'archivio gli atti, i documenti e i supporti, non più necessari per la svolgimento delle proprie mansioni lavorative.
Per quanto concerne l'archiviazione, il Titolare ha adibito apposite aree nelle quali conservare ordinatamente documenti, atti e supporti contenenti dati personali.
L'archiviazione di documenti, atti e supporti contenenti dati particolari (cosiddetti ex sensibili, ex giuridici, ecc.) avviene in luoghi e armadi che sono normalmente chiusi e controllati.
L'accesso a tali archivi è consentito solo alle persone incaricate del trattamento ed è controllato tramite richiesta della chiave all'incaricato che ha il compito di custodirla.
È previsto l'uso di dispositivi distruggi documenti per tutti i documenti errati stampati per errore o il cui uso non risulti più attinente alle finalità in indicate o non sia giustificato.
Gli impianti e le attrezzature, di cui e dotato il Titolare per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati particolari (cosiddetti ex sensibili, ex giuridici, ecc.) appaiono:

- soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali contenuti in tali atti, documenti e supporti;
  Per l'anno 2019, sono previsti interventi di manutenzione e/o di rimpiazzo;
- nel medio periodo è previsto l'adeguamento/miglioramento tecnologico a base di Norma.

I.3 Le misure logiche di sicurezza

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- realizzazione e gestione di un sistema di autenticazione informatica che ha il fine di accertare l'identità delle persone affinché a ogni strumento elettronico possa accedere solo chi e autorizzato;
- realizzazione e gestione di un sistema di autorizzazione che ha il fine di circoscrivere, le tipologie di dati ai quali gli incaricati possono accedere e i trattamenti che possono effettuare, da quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative;
- realizzazione e gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus);
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (Floppy disk, dischi ZIP, CD, dischi usb, pen-drive, ecc.) nei quali siano contenuti dati personali;
- implementazione di un sistema di protezione di tipo firewall ove previsto dal sistema operativo;
- aggiornamento degli strumenti e dei programmi informatici utilizzati.

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;
- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

L'eccezione vale, ovviamente, solo per gli strumenti elettronici che non siano in rete, o che siano in rete esclusivamente con strumenti elettronici non contenenti dati personali, o contenenti solo dati personali destinati alla diffusione.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere a un determinato strumento elettronico.
Per realizzare le credenziali di autenticazione si utilizza il seguente metodo:

- si associa un codice per identificazione dell'incaricato (username), attribuito da chi amministra il sistema, a una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà a elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- a ogni incaricato esse vengono assegnate o associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziate;
- il codice per l'identificazione (username), è attribuito all'incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri incaricati, neppure in tempi diversi;
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'incaricato perda la qualità che gli consentiva di accedere alto strumento;
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- dovere di elaborare in modo appropriato la password e di conservare la segretezza sulla stessa nonché sulle altre componenti riservate della credenziale di autenticazione (username), attribuite dall'amministratore di sistema.
  Agli incaricati è imposto l'obbligo di provvedere a modificare la password con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - successivamente, almeno ogni tre mesi.

  Le password sono composte da almeno otto caratteri.
  Agli incaricati e prescritto di utilizzare alcuni accorgimenti, nell'elaborazione delle password:
  - esse non devono contenere riferimenti agevolmente riconducibili all'interessato (non solo nomi, cognomi, soprannomi, ma neppure date di nascita proprie, dei figli o degli amici), ne consistere in nomi noti, anche di fantasia;
  - buona norma è che, dei caratteri che costituiscono la password, da un quarto alla metà siano di natura numerica e che siano caratteri maiuscoli e minuscoli.

  La password non deve essere comunicata a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, responsabili del trattamento, amministratore del sistema o titolare).
  Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe però rendersi necessario disporre della password dell'incaricato per accedere agli strumenti e ai dati.
  A tale fine agli incaricati sono state fornite istruzioni scritte, affinché essi:
  - scrivano la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata;
  - consegnino la busta a chi custodisce le copie delle parole chiave il cui nominativo viene loro indicato al momento dell'attribuzione della password.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Solo al verificarsi delle condizioni sopra esposte, che rendono necessario accedere allo strumento elettronico utilizzando la copia della parola chiave, il titolare o un responsabile potranno richiedere la busta che la contiene a chi la custodisce.
Dall'accesso effettuato si dovrà procedere a informare, tempestivamente, l'incaricato cui appartiene la parola chiave.

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, e i trattamenti che possono effettuare si osserva che si è impostato un sistema di autorizzazioni al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere e i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative.
Ove possibile il Titolare del trattamento ha provveduto a cifrare i dati non più trattati e/o quelli contenenti dei dati personali particolari (cosiddetti ex sensibili, ex giuridici, ecc.).
L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.
Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal responsabile, ovvero da soggetti da questi appositamente incaricati.
Periodicamente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.
Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

- Il primo aspetto riguarda la protezione dei dati personali dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).
  A tale fine si è dotati di idonei strumenti elettronici e programmi sono sottoposti ad aggiornamento, di regola, ogni volta che sono disponibili aggiornamenti.
  Tutti gli incaricati sono stati istruiti in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere per minimizzare il rischio di essere contagiati: a tale fine è stato loro distribuito un codice dei comportamenti da tenere e di quelli da evitare (manuale sulla sicurezza).

- Il secondo aspetto riguarda la protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.
  La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall.

- Il terzo aspetto riguarda l'utilizzo di appositi programmi la cui funzione è di prevenire la vulnerabilità degli strumenti elettronici tramite la verifica di eventuali inconsistenze e inesattezze nella configurazione dei sistemi operativi e dei servizi di rete e di correggere, di conseguenza, i difetti insiti negli strumenti stessi.
  A tale riguardo vale quanto indicato in precedenza nel senso che periodicamente si verifica la presenza di aggiornamenti o patch relativi ai software utilizzati dal Titolare. L'installazione di tali aggiornamenti o patch viene di volta in volta decisa dal responsabile dei sistemi informativi (o dall'Amministratore di Sistema o dal Titolare) in fusione della propria esperienza.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Per quanto concerne i supporti rimovibili (es. floppy disk, dischi ZIP, CD, HD USD, ecc.), contenenti dati personali la norma impone particolari cautele sono nell'ipotesi in cui essi contengano dati personali particolati (sensibili, giudiziari, ecc.).
Il Titolare ha ritenuto di estendere tali precetti ai supporti contenenti dati personali di qualsiasi natura, anche comune, prescrivendo agli incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare essi devono essere conservati in cassetti chiusi a chiave durante il loro utilizzo e successivamente formattati quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;

- una volta cessate le ragioni per la conservazione dei dati si devono in ogni caso porre in essere gli opportuni accorgimenti finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supportarti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

I.4 Dispositivi mobili

Per quanto riguarda l'uso di dispositivi mobili (Notebook, smartphone, ecc.) l'azienda ha formato il personale per renderlo edotto sul come gestire tali dispositivi ed ha messo in essere l'uso di procedure di crittografazione che rendono illeggibili i dati in essi contenuti. Solo le persone incaricate e autorizzate possono utilizzare "in chiaro" tali dispositivi.

I.5 Ulteriori misure adottate

I dati sono trattati esclusivamente all'interno di locali protetti accessibili ai solo incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi.
Non è previsto nessun trasporto di dati all'esterno dei locali riservati al loro trattamento; in caso di necessità tale trasporto sarà fatto in contenitori muniti di serratura o dispositivi equipollenti.
Il trasporto di dati in formato elettronico avviene solamente dopo l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

I.6 Trattamento senza l'ausilio di strumenti elettronici

- Per quanto riguarda i trattamenti fatti senza l'ausilio di strumenti elettronici agli incaricati il Titolare ha impartito istruzioni scritte finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali, Periodicamente, con cadenza almeno annuale, si verifica l'ambito del trattamento consentito ai singoli incaricati.
- Tutti gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera tale che ad essi non accedano persone price di autorizzazione e sono restituiti al termine delle operazioni affidate.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- L'accesso agli archivi contenenti dati sensibili è controllato. Non sono ammesse persone dopo l'orario di chiusura. Eventuali accessi dopo l'orario di chiusura sono preventivamente autorizzati e registrati in un apposito modello allegato al presente documento.
- Agli archivi vi accedono solo persone preventivamente autorizzate.
- È previsto l'uso di dispositivi distruggi documenti per tutti i documenti errati, stampati per errore o il cui uso non risulti più attinente alle finalità indicate o non si a più giustificato.

  In considerazione di quanto disposto dal Disciplinare Tecnico in materia di misure minime di sicurezza si precisa che a tutti gli incaricati è fatto divieto di:
  - effettuare copie su supporti magneti o trasmissioni non autorizzate dal Titolare del trattamento;
  - effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare del trattamento, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto di trattamento;
  - sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare del trattamento, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto di trattamento;
  - consegnare a persone non autorizzate dal Titolare del trattamento, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto di trattamento.

In aggiunta a quanto indicato precedentemente di seguito elenchiamo il piano di trattamento dei rischi redatto dal Titolare del trattamento (vedere allegato 4).

I.7 Ricapitolando

Le misure logiche di sicurezza, di cui è dotato il Titolare per la protezione dei trattamenti che avvengono con strumenti elettronici appaiono nel loro complesso soddisfacenti, al fine di garantire la necessaria sicurezza ai dati personali trattati, anche per i dati particolari (cosiddetti ex sensibili ora art. 9 punto 1 Regolamento EU, ex giuridici ora art. 10 Regolamento UE, ecc.).
Quindi risultano verificati e abbattuti allo stato attuale i rischi significativi per i diritti e la libertà fondamentali della persona, i rischi di distruzione accidentale o illegale, i rischi di perdita dei dati, i rischi di modifica non voluta, il rischio di comunicazione e diffusione non consentita. Per l'anno 2019, sono quindi previsti semplicemente interventi finalizzati all'aggiornamento, alla manutenzione e a qualche rimpiazzo.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

J. Criteri e modalità di ripristino dei dati (la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento)

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità di tali da garantire il loro ripristino in termini ragionevoli e comunque entro una settimana per i dati particolari (cosiddetti ex sensibili ora art. 9 punto 1 Regolamento UE, ex giuridici ora articolo 10 Regolamento EU, ecc.).
Per ridurre considerevolmente la probabilità di perdita di dati dovuta a cattivo funzionamento dei rischi fissi sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia, su dispositivi opportuni, di tutti i dati registrati. Allo scopo si utilizza:

- un NAS sul quale vengono effettuate copie di sicurezza giornaliere;
- un hard disk esterno che viene collegato al NAS.

Considerato che i salvataggi sono sempre effettuati in modo totale e non incrementale, il ripristino della disponibilità dei dati (restore) avviene in modo inverso a come viene effettuato il salvataggio (backup).

La seguente tabella riassume le modalità adottate per il salvataggio e i ripristino dei dati.

Banca dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino	Struttura incaricata del salvataggio
Tutte le banche dati e le cartelle personali	NAS + hard disk esterno Periodicità: ogni giorno	Ogni mese	Addetto alle copie di Sicurezza

Vista la metodologia applicata e le procedure utilizzate per la realizzazione e gestione delle copie di sicurezza si può dire che il ripristino dei dati in caso di danneggiamento degli stessi o degli strumenti elettronici risulta compatibile con i diritti degli interessati e realizzabile in tempi brevi.

J.1 Pianificazione degli interventi formativi previsti

Sono previsti interventi formativi degli incaricati del trattamento, finalizzati a rendere edotti i Soggetti Incaricati dei seguenti aspetti:

- ✓ profili della disciplina sulla protezione dei dati personali che appaiono più rilevanti per l'attività svolta degli incaricati e delle conseguenti responsabilità che ne derivano;
- ✓ rischi che incombono sui dati;
- ✓ misure disponibili per prevenire eventi dannosi;
- ✓ modalità per aggiornarsi sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale da avere luogo al verificarsi di una delle seguenti circostanze:

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

- ✓ al momento dell'ingresso in servizio;
- ✓ in occasione di cambiamenti di mansioni che implicano modifiche rilevanti rispetto al trattamento di dati personali;

- ✓ in occasione dell'introduzione di nuovi significativi strumenti che implicano modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del responsabile per la sicurezza o gi altri soggetti esperti nella materia, che all'esterno presso soggetti specializzati.

La seguente tabella riporta la pianificazione degli interventi previsti

Descrizione sintetica degli interventi formativi	Strutture interessate	Tempi previsti
- Introduzione al Regolamento Europeo n. 679/2016, rischi incombenti sui dati, misure disponibili per prevenire eventi dannosi sui dati, adozione delle misure minime di sicurezza adottate, distinzione tra tipi di dati personali. - Modalità di gestione dei dati Personali particolari (cosiddetti ex sensibili ora articolo 9 punto 1 Regolamento UE, ex giuridici ora articolo 10 Regolamento UE). - Variazione password. - Salvataggio dati e utilizzo delle Cartelle Personali. - Comportamenti da adottare per prevenire "Infezioni" da virus. - Rischi connessi all'uso della posta elettronica. - Rischi connessi all'uso di internet.	Tutte (Direzione, amministrazione, ecc.)	Un'ora

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

K. L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Regolamento Europeo n. 679/2016, all'esterno della struttura del Titolare, si adottano i seguenti criteri atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime previste dal regolamento stesso:

1. Qualora un trattamento debba essere effettuano per contro del Titolare del trattamento della presente Azienda, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento Europeo n. 679/2016 e garantisca la tutela dei diritti dell'interessato.

2. Il titolare del trattamento impartisce ai Responsabili del trattamento di non ricorre a un altro Responsabile senza previa autorizzazione scritta, specifica o generale. Nel caso di autorizzazione scritta generale, il Titolare del trattamento chiede al Responsabile del trattamento di essere informato di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, avendo così l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il Responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il Responsabile del trattamento nominato:
   a. tratti i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento; in tal caso, il Responsabile del trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico:
   b. garantisca che le persone autorizzate al trattamento dei dati personali si siano impiegante alla riservatezza o abbiamo un adeguato obbligo legale di riservatezza;
   c. adotti tutte le misure richieste ai sensi dell'articolo 32;
   d. rispetti le condizioni di cui ai punti 2 e 4 sopra indicati per ricorrere a un altro Responsabile del trattamento;
   e. tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguare, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.
   f. assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo n. 679/2016, tenendo contro della natura del trattamento delle informazioni a disposizione del Regolamento del trattamento;
   g. su scelta del Titolare del trattamento, cancelli i gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento o cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
   h. metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente documento e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

   Il Responsabile per trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione di quelle precedentemente date violi il Regolamento Europeo n. 679/2016 o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per contro del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione di dati contenuti nel contratto o in altro atto giuridico tra il

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

Titolare del trattamento e il Responsabile del trattamento di cui al paragrafo 3 sopra indicato, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento Europeo n. 679/2016. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile del trattamento

5. L'adesione da parte del Responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 del Regolamento Europeo n. 679/2016 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente testo.

6. Fatto salvo un contratto individuale tra il Titolare del trattamento e il Responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente documento può basarsi, in tutto o in parte, anche laddove siano parte di una certificazione concessa al Titolare del trattamento o al Responsabile del trattamento, ai sensi degli articoli 42 e 43 del Regolamento Europeo n. 679/2016.

Il Titolare del trattamento della scrivente avvisa il Responsabile del trattamento che, fatti salvi gli articoli 82, 83 e 84 del Regolamento Europeo n. 679/2016, se un Responsabile del trattamento viola le indicazioni impartite, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

K.1 Trattamenti affidati all'esterno

Descrizione dell'attività esternalizzate	Trattamenti interessati	Soggetto esterno	Criteri e impegni assunti per l'adozione delle misure
Direzione e Coordinamento Espletamento adempimenti amministrativi. Gestione Contabile e Finanziaria	T1 Dati comuni relativi a clienti T2 Dati comuni relativi a fornitori T3 Dati comuni relativi ad altri soggetti T4 Dati di natura economico-finanziaria relativi al Titolare. T5 Dati personali relativi ai Soci, agli Amministratori	Studio Commercialista	Nomina a Responsabile Esterno del trattamento

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

L. Controllo generale sullo stato della sicurezza

Al Titolare del trattamento è affidato il compito di aggiornare le misure di sicurezza al fine di adottare gli strumenti e le conoscenze resi disponibili dal progresso tecnico che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.
Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Titolare del trattamento e le persone da questo appositamente incaricate provvedono con frequenza mensile, anche con controlli a campione, ed effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia e il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log. file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete (controllo agg. Antivirus, firewall, ecc.);
- verificare che i supporti magnetici, che non possono più essere utilizzati, vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni tre mesi si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.
Dall'attività di verifica svolta viene redatto un verbale, che viene conservato dal Titolare.

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916

M. Dichiarazioni d'impegno e firma

Il presente documento, redatto nel mese di luglio 2019, viene firmato in calce da Marzenta Anna Maria, in qualità di Titolare del trattamento.
L'originale del presente documento viene custodito presso la sede dell'Azienda per essere esibito in caso di controlli.
Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

Ponte San Nicolò, _____

Firma del titolare del Trattamento

_____

Via Monte Sabotino, 12/A 35020 Ponte San Nicolò (Padova) Tel. 049- 8962825
e-mail: info@cometaasmme.org www.cometaasmme.org
Reg. Vol. Regione Veneto PD 222 – C/C Postale: 15114358 – C/C Bancario: IBAN IT19X0306962603074000290916