



MODELLO DI ORGANIZZAZIONE E DI GESTIONE
ai sensi del D.lgs. 8 giugno 2001 n. 231 della società
ASTEM S.p.A.

Parte speciale

Protocollo
Reati informatici e di trattamento illecito di dati

Rev. dicembre 2024

Sommario

1. Premesse	3
2. Elenco dei delitti informatici e di trattamento illecito di dati previsti dal d.lgs 231/2001	4
3. Funzione della parte speciale - delitti informatici e di trattamento illecito di dati	12
4. Principi di riferimento generali	13
4.1. Il sistema organizzativo in generale	13
4.2. Principi generali di comportamento	14
5. Le attività sensibili ai delitti informatici e di trattamento illecito di dati ai fini del d.l.231/01	16
5.1. Principi generali di controllo	16
6. Principi di riferimento relativi alla regolamentazione delle singole attività sensibili	17
7. I controlli dell'Organismo di Vigilanza	21
8. Diffusione e informazione	22
9. Sanzioni	23

1. PREMESSE

Il presente Protocollo si riferisce ai reati informatici e in tema di trattamento illecito di dati. L'individuazione delle "aree di attività a rischio" ha rappresentato un'attività fondamentale per la costruzione del Modello di Organizzazione, Gestione e Controllo di ASTEM S.p.A..

Con specifico riferimento ai reati informatici e in tema di trattamento illecito di dati, l'analisi del contesto aziendale di ASTEM S.p.A. ha consentito di identificare:

- (i) i potenziali reati associabili ad attività aziendali ritenute sensibili;
- (ii) le macroaree aziendali e i settori di attività ritenuti sensibili nonché gli ambiti, le funzioni, le attività e i processi a rischio reato (ossia quelle aree, funzioni, uffici, unità organizzative aziendali, processi, ecc. che pongono in essere attività critiche ed a rischio rilevanti ai fini della possibile commissione dei reati previsti nel Decreto 231);
- (iii) i potenziali enti pubblici coinvolti (a livello esemplificativo);
- (iv) le possibili modalità di realizzazione del reato e le possibili finalità della condotta illecita.

In proposito, per esigenze di brevità, si rinvia al documento "Mappatura delle Aree Aziendali Sensibili".

2. ELENCO DEI DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI PREVISTI DAL D.LGS 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. 231/2001 è collegato il regime di responsabilità a carico della società, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

A tal fine, si riporta di seguito una descrizione dei reati richiamati dall'art. 24-bis del d.lgs. 231/2001.

Delitti informatici e trattamento illecito di dati (Art. 24-bis, D.Lgs. n. 231/2001)

Falsità in un documento informatico pubblico o avente efficacia probatoria (art. 491-bis c.p.) – “Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici e le scritture private”

Questo reato si realizza nel caso di compimento di una condotta illecita di falso relativamente a documenti informatici pubblici o privati aventi efficacia probatoria. In particolare, le falsità concernenti documenti e atti informatici rilevano ai fini del d. lgs. 231/2001, se riferite alle disposizioni indicate dal capo stesso e riferite agli atti pubblici e alle scritture private, che per semplicità, si riportano di seguito.

- **art. 476 c.p. - falsità materiale commessa dal pubblico ufficiale in atti pubblici:** vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.
- **art. 477 c.p. - falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative:** vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.
- **art. 478 c.p. - falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti:** vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni. Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni. Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.
- **art. 479 c.p. - falsità ideologica commessa dal pubblico ufficiale in atti pubblici:** vi incorre il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476
- **art. 480 c.p. - falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative:** vi incorre il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.
- **art. 481 c.p. - falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità:** vi incorre chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da Euro 51,00 a Euro 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.
- **art. 482 c.p. - falsità materiale commessa dal privato:** se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.
- **art. 483 c.p. - falsità ideologica commessa dal privato in atto pubblico:** vi incorre chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni. Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.
- **art. 484 c.p. - falsità in registri e notificazioni:** vi incorre chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa

circa le proprie operazioni industriali, commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a Euro 309,00.

- **art. 485 c.p. - falsità in scrittura privata:** vi incorre chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.
- **art. 486 c.p. - falsità in foglio firmato in bianco. atto privato:** vi incorre chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.
- **art. 487 c.p. - falsità in foglio firmato in bianco. atto pubblico:** vi incorre il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.
- **art. 488 c.p. - altre falsità in foglio firmato in bianco. applicabilità delle disposizioni sulle falsità materiali:** casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private.
- **art. 489 c.p. uso di atto falso:** vi incorre chiunque senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo. Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.
- **art. 490 c.p. soppressione, distruzione e occultamento di atti veri:** vi incorre chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente.
- **art. 492 c.p. copie autentiche che tengono luogo degli originali mancanti:** agli effetti delle disposizioni precedenti, nella denominazione di "atti pubblici" e di "scritture private" sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.
- **art. 493 c.p. - falsità commesse da pubblici impiegati incaricati di un servizio pubblico:** le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

*

Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) – “[1] Chiunque abusivamente si introduce 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, è punito con la reclusione fino a tre anni.

[2] La pena è della reclusione da due a dieci anni:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 2) se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 3) se dal fatto deriva la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

[3] Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni.

[4] Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio”.

Questo reato si realizza tramite la condotta di un soggetto che 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- per la fattispecie sopracitata, la pena è generalmente della reclusione fino a tre anni e il delitto si punisce a querela della persona offesa;
- la pena è, invece, della reclusione da uno a cinque anni e si procede d'ufficio:
 - 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
 - 2) se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;
 - 3) se dal fatto deriva la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti;

I numeri 2 e 3 del comma 2 sono stati modificati dalla legge 90/2024 che ha altresì inasprito le pene previste dalla norma

*

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) – “*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.*

La pena è della reclusione da due anni a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma”.

La fattispecie si concretizza allorché un soggetto, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque.

Il bene giuridico oggetto di tutela è la riservatezza informatica e la indisturbata fruizione del sistema informatico da parte del gestore.

La norma punisce una condotta prodromica alla commissione del delitto di cui all'articolo 615 ter, sanzionando infatti la detenzione o la messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela del "domicilio informatico altrui".

Viene ad ogni modo richiesto il dolo specifico costituito dal fine di procurarsi un profitto, di danneggiare o di permettere il danneggiamento o comunque il non funzionamento (anche temporaneo) di un sistema informatico.

Per sistema informatico va inteso un insieme di apparecchiature destinate a compiere una funzione utile all'uomo attraverso il ricorso a tecnologie informatiche.

*

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) – “*Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico*

o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da quattro a dieci anni; se il fatto è commesso:

- 1) in danno di taluno dei sistemi informatici o telematici indicati nell'articolo 615 ter, terzo comma;
- 2) in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
- 3) [ABROGATO].

Tale reato consiste nell'intercettazione, nell'impedimento o nell'interruzione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione da sei mesi a cinque anni; salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle sopracitate comunicazioni;
- i delitti sono punibili a querela della persona offesa.

Tuttavia, si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso:

- 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema.

*

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) –

“Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni”.

Questo reato condanna la condotta di quei soggetti che, fuori dai casi consentiti dalla legge, installano apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque.

*

Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.) –*“[1] Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni.*

[2] La pena è della reclusione da tre a otto anni:

- 1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
- 2) *se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato”.*

Il reato condanna la condotta dei soggetti che distruggono, deteriorano, cancellano, alterano o sopprimono informazioni, dati o programmi informatici altrui.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la fattispecie aggravata è stata modificata dalla Legge 90/2024 che ha altresì inasprito le pene previste dalla norma.

*

Danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.) – *“Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all’ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, è punito con la reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:

- 1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
- 2) *se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;*
- 3) *se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l’alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l’inaccessibilità al legittimo titolare dei dati o dei programmi informatici.*

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)”.

Tale condotta criminosa consiste nella commissione di un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici pubblici o di interesse pubblico.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque.

*

Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.) – *“Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all’articolo 635-bis, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da due a sei anni.*

La pena è della reclusione da tre a otto anni:

- 1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
- 2) *se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato”.*

Tale delitto punisce la condotta del soggetto che, mediante le condotte di cui all’art. 635-bis, ovvero attraverso l’introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque.

*

Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.) – *“Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.*

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.”.

La legge 90/2024 ha abrogato l'art. 615-quinquies e riprodotto al comma 1 dell'art. 635 quater.1 c.p. la medesima fattispecie

Il bene giuridico oggetto di tutela è la riservatezza informatica e la indisturbata fruizione del sistema informatico da parte del gestore.

La norma punisce una condotta prodromica alla commissione del delitto di cui all'articolo 615 ter, sanzionando infatti la detenzione o la messa a disposizione di apparecchiature in grado di infrangere i presidi posti a tutela del "domicilio informatico altrui".

Viene ad ogni modo richiesto il dolo specifico costituito dal fine di danneggiare o di permettere il danneggiamento o comunque il non funzionamento (anche temporaneo) di un sistema informatico.

Per sistema informatico va inteso un insieme di apparecchiature destinate a compiere una funzione utile all'uomo attraverso il ricorso a tecnologie informatiche.

La legge 90/2024 ha inoltre introdotto delle fattispecie aggravate ai commi 2 e 3.

*

Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.) –

“Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

- 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
- 2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;*
- 3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.*

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3)”.

Strutturalmente questa ipotesi criminosa è simile a quella trattata al punto precedente, ad eccezione del fatto che le sopraccitate condotte sono dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Si tratta di reato comune, la cui condotta può essere realizzata da chiunque, salve le ipotesi aggravate del co. 2.

Le pene sono state inasprite dalla legge 90/2024.

*

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-

quinquies c.p.) – *“[1] Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla*

legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro"

Il reato si concretizza qualora il soggetto che presta servizi di certificazione di firma elettronica il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Si precisa che la pena è della reclusione fino a tre anni e della multa da 51 a 1.032 euro.

*

Reato di ostacolo o condizionamento dei procedimenti per la Sicurezza Cibernetica e delle relative attività ispettive e di vigilanza (articolo 1 co. 11 D.lgs 105/2019) – *“Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni”.*

Il reato si concretizza con la fornitura di dati non corrispondenti al vero al fine di ostacolare le procedure connesse alla sicurezza Cibernetica come meglio definite nella norma citata e gestite dall'Agenzia per la cybersicurezza nazionale, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la cybersicurezza; il Dipartimento delle informazioni per la sicurezza, l'Agenzia informazioni e sicurezza esterna (AISE) e l'Agenzia informazioni e sicurezza interna (AISI).

*

Estorsione informatica (art. 629 co. 3 c.p.c. come modificato dall'art. 16, comma 1, lettera m) della L. 28 giugno 2024, n. 90) - *“Chiunque, mediante le condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità”.*

Il resto è stato introdotto dall'art. 16, comma 1, lettera m) della L. 28 giugno 2024, n. 90, che ha disposto la modifica del comma 2 e l'introduzione di un comma 3.

Trattasi di una fattispecie specifica di estorsione commessa attraverso i reati (anche se solamente minacciati) di:

- accesso abusivo a sistema informatico o telematico;
- danneggiamento di informazioni, dati e programmi informatici;
- danneggiamento di sistemi informatici o telematici;
- danneggiamento di sistemi informatici o telematici di pubblica utilità;
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche;
- falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche.

L'ipotesi aggravata ricorre se:

- la violenza o minaccia è commessa con armi o da persona travisata, o da più persone riunite;
- la violenza o minaccia è posta in essere da persona che fa parte di un'associazione per delinquere di tipo mafioso;
- il fatto sia commesso nei confronti di persona incapace per età o per infermità;
- la violenza consiste nel porre taluno in stato di incapacità di volere o di agire.

Esistono anche delle circostanze attenuanti, previste all'art. 639-ter c.p.:

- la pena è diminuita fino ad un terzo quando, per la natura, la specie, i mezzi, le modalità o le circostanze dell'azione ovvero per la particolare tenuità del danno o del pericolo, il fatto risulti di lieve entità;

- la pena è diminuita dalla metà a due terzi per chi si adopera per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, anche aiutando concretamente l'autorità di polizia o l'autorità giudiziaria nella raccolta di elementi di prova o nel recupero dei proventi del delitto o degli strumenti utilizzati per la commissione dello stesso.

A seguito dell'entrata in vigore della legge cybersicurezza costituisce reato-presupposto soltanto l'estorsione qualificata da una particolare modalità di condotta, quella integrante le fattispecie di reato informatico sopra menzionate.

La legge vuole intervenire in maniera decisa sulla c.d. *cyber extortion*, che si propone di bloccare o limitare le funzioni di un dispositivo finché non si paga un riscatto.

Si può trattare, per esempio, di divulgazione di informazioni sensibili dei dipendenti di un'azienda o dei suoi clienti ovvero di dati confidenziali che, se divulgati, potrebbero danneggiare la reputazione di un soggetto o di un'azienda.

Il nuovo reato di estorsione informatica viene inserito, dunque, all'art 24-bis d.lgs. 231/2001, e potrebbe condurre all'affermazione di responsabilità dell'ente a vantaggio del quale viene commessa, oltre all'applicazione della sanzione pecuniaria da 300 a 800 quote e delle sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni.

Generalmente in relazione all'estorsione informatica è normale pensare all'azienda in qualità di vittima; tuttavia, è altresì possibile, ed anzi probabile, che sussista una finalità di vantaggio concorrente dell'ente, ad esempio, quando la condotta ha lo scopo accedere abusivamente al sistema informatico di un concorrente.

La durata delle sanzioni interdittive è prevista in misura non inferiore a due anni, che equivale alla durata massima delle interdittive secondo il d.lgs. 231/2001: nemmeno per reati gravi quali i delitti di criminalità organizzata e i delitti contro la personalità individuale è prevista una sanzione così rigida.

3. FUNZIONE DELLA PARTE SPECIALE - DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai Dipendenti, nonché dai Consulenti, come meglio definiti nella parte generale, coinvolti nelle Fattispecie di attività sensibili.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.

Nella parte generale sono stati richiamati i principi ispiratori della normativa e i presidi principali per l'attuazione delle vigenti disposizioni in materia.

In questa parte speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione alle fattispecie di attività sensibili individuate al fine di prevenire la commissione dei delitti informatici e di trattamento illecito di dati.

4. PRINCIPI DI RIFERIMENTO GENERALI

4.1. Il sistema organizzativo in generale

Nell'espletamento di tutte le operazioni direttamente o indirettamente attinenti alla gestione e all'utilizzo dei sistemi informativi aziendali, i Dipendenti e gli Organi Sociali devono adottare e rispettare:

- 1) il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;
- 2) le norme inerenti il sistema amministrativo, contabile, finanziario e controllo di gestione di ASTEM S.p.A.;
- 3) il sistema disciplinare;
- 4) in generale, la normativa applicabile.

In particolare, ai fini del presente Protocollo, si recepiscono tutte le regole e tutti i principi contenuti nei seguenti documenti che devono intendersi, pertanto, qui integralmente trascritti:

- a) le disposizioni legislative e regolamentari, italiane o straniere, applicabili alla fattispecie;
- b) le previsioni dello Statuto sociale;
- c) il Codice etico;
- d) le norme generali emanate ai fini del D.Lgs. 231/01;
- e) le verbalizzazioni, le deliberazioni e le eventuali risoluzioni degli organi previsti dai sistemi di Governance in essere;
- f) le procedure interne introdotte dal modello organizzativo e necessarie a mitigare il rischio di reato;
- g) le disposizioni di servizio (circolari) emanate dalle unità organizzative competenti e dai superiori gerarchici;
- h) il progetto di protezione dati personali adottato dalla società.

Si precisa che ASTEM S.p.A. ha nominato:

- un responsabile unico interno per il trattamento dati personali;
- un responsabile per la Protezione dei Dati personali o Data Processor Officer (RPD-DPO);
- una società esterna che svolge funzioni di referente IT;

al fine di meglio garantire la gestione dei sistemi informativi aziendali, l'implementazione, il monitoraggio e la corretta applicazione delle relative procedure di controllo, nonché in ultima analisi la protezione dei dati.

Inoltre, con particolare riferimento:

- alla piattaforma di E-Procurement;
- alla piattaforma Whistleblowing;

accessibili tramite link presente sul sito web della società, in virtù degli accordi contrattuali in essere tra le parti, al fine di presidiare l'attività sensibile in oggetto, il service provider, su indicazioni specifiche di ASTEM S.p.A., adotta tutte le misure di cui al successivo paragrafo, garantendo piena conformità dei servizi erogati rispetto ai criteri stabiliti all'interno dei contratti ed essendo pertanto responsabile di eventuali inadempienze.

4.2. Principi generali di comportamento

La presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali (in via diretta) e dei lavoratori dipendenti e dei consulenti di ASTEM S.p.A. (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che - considerati individualmente o collettivamente - integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del d.lgs. 231/2001);
- violare i principi e le procedure aziendali applicabili alla presente parte speciale.

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di:

- 1) impegnarsi a non rendere pubbliche tutte le informazioni loro assegnate per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password, anche se superata, necessaria per l'accesso ai sistemi dell'Azienda);
- 2) attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione (uscita dal sistema o blocco dell'accesso tramite password);
- 3) accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere, entro le scadenze indicate dal Responsabile IT Governance, alla modifica periodica della password;
- 4) astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;
- 5) assicurare la veridicità delle informazioni contenute in qualsivoglia atto e/o documento informatico.

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

- a) intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;
- b) installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile IT Governance;
- c) accedere alla rete aziendale attraverso una connessione alternativa rispetto a quella messa a disposizione da parte dell'Azienda, al fine di eludere il sistema di accesso protetto implementato;
- d) accedere in maniera non autorizzata ai sistemi informativi di terzi, né alterarne in alcun modo il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse di ASTEM S.p.A., i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;
- contenere clausole standard al fine del rispetto del Regolamento UE 2016/679 e

del D. Lgs. 196/2003 garantendo il medesimo livello di protezione e sicurezza dei dati personali che deve essere garantito da ASTEM S.p.A.;

- contenere clausole standard al fine del rispetto del D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto);
- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti conformi al dettato della norma;
- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es. clausole risolutive espresse, penali).

5. LE “ATTIVITÀ SENSIBILI RELATIVE AI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI” AI FINI DEL D.LGS. 231/2001

Le attività sensibili individuate, in riferimento ai Delitti informatici e di trattamento illecito di dati richiamati dall'art. 24-bis del d.lgs. 231/2001, sono le seguenti:

- (i) **Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato “Gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici” e “Invio telematico di atti, documenti e scritture”);**
- (ii) **Invio di newsletter;**
- (iii) **Navigazione sul sito web aziendale;**
- (iv) **Utilizzo e gestione della piattaforma E-Procurement;**
- (v) **Utilizzo e gestione della piattaforma Whistleblowing;**
- (vi) **Utilizzo e gestione degli altri software e piattaforma in uso all'azienda.**

5.1. Principi generali di controllo

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- **segregazione delle attività:** si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;
- **esistenza di procedure/norme/circolari:** devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;
- **poteri autorizzativi e di firma:** i poteri autorizzativi e di firma devono:
 - (i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese;
 - (ii) essere chiaramente definiti e conosciuti all'interno della Società;
- **tracciabilità:** ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

6. PRINCIPI DI RIFERIMENTO SPECIFICI RELATIVI ALLE REGOLAMENTAZIONE DELLE SINGOLE ATTIVITÀ SENSIBILI

Ai fini dell'attuazione delle regole elencate al precedente paragrafo 4, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al precedente paragrafo 5.1, nel disciplinare le fattispecie di attività sensibili di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

- (i) ***Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato "Gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici" e "Invio telematico di atti, documenti e scritture")***;

La regolamentazione dell'attività deve prevedere:

- l'implementazione di un approccio di governance dei sistemi informativi aziendali improntato al rispetto degli standard di sicurezza attiva e passiva, volti a garantire l'identità degli utenti e la protezione, la confidenzialità, l'integrità e la disponibilità dei dati. In particolare, ASTEM S.p.A. ha implementato un sistema centralizzato per la gestione delle componenti software, che, pertanto, non possono essere aggiornate o modificate in alcun modo da parte del singolo utente;
- la possibilità di accedere ai sistemi informativi solo previa opportuna identificazione da parte dell'utente, a mezzo username e password assegnati originariamente dall'Azienda. Per i sistemi di identificazione e accesso ASTEM S.p.A. ha definito un iter tale per cui ogni utente ha necessità di inserire una password - costituita da un codice alfanumerico con un numero minimo di caratteri - per "loggarsi" e accedere ai sistemi;
- l'obbligo di cambiamento della password, a seguito del primo accesso, e la periodicità di modifica della suddetta password a seconda della frequenza di utilizzo e della criticità dei dati cui si accede per mezzo della stessa. In particolare, il sistema informativo di ASTEM S.p.A. prevede che ciascun utente modifichi la propria password periodicamente e comunque non oltre 90 giorni dalla registrazione. Qualora l'utente non provveda alla modifica di propria iniziativa, il sistema è strutturato in modo da inviare in automatico alert preliminari alcuni giorni prima che la password scada. Decorso anche questo termine, il sistema obbliga l'utente al cambio password per poter accedere al sistema;
- il monitoraggio, con frequenza periodica, di tutti gli accessi e le attività svolte sulla rete aziendale nei limiti e con le modalità di cui alla vigente normativa.
- ASTEM S.p.A. prevede una lista con un elenco dettagliato di siti inaccessibili ai propri utenti;
- la registrazione e la verifica di tutti gli accessi e le attività svolte sulla rete aziendale da remoto, nei limiti e con le modalità di cui alla vigente normativa. In particolare, gli utenti autorizzati da ASTEM S.p.A. hanno la possibilità di accedere alla rete da remoto tramite check-point VPN - previa espressa autorizzazione del Responsabile gerarchico, oppure utilizzando esclusivamente la mail, con

l'autorizzazione del Responsabile gerarchico e dopo aver seguito un corso sulla sicurezza informatica;

- Inoltre, l'Ufficio del Personale comunica tutte le assunzioni e le cessazioni, nonché tutti i passaggi di stato/mansioni che possono impattare sulla gestione delle utenze informatiche, in modo che vengano attivate tutte le utenze necessarie. Si sottolinea che, al fine di abilitare le utenze, è necessaria l'autorizzazione del diretto superiore dell'utente richiedente;
- La cessazione dei rapporti lavorativi comporta la disattivazione delle utenze e l'approntamento di un messaggio di avviso della disattivazione della casella con indicazione dell'indirizzo a cui inoltrare le comunicazioni. Non viene applicato alcun *redirect* ad altra casella;
- l'adeguata formazione di ogni risorsa sui comportamenti da tenere per garantire la sicurezza dei sistemi informativi e sulle possibili conseguenze, anche penali, che possono derivare dalla commissione di un illecito.

Per la gestione adempimenti in materia di tutela della privacy, ASTEM S.p.A., nel rispetto di quanto stabilito dal D. Lgs. 196/2003:

- predispone idonee informative al fine di acquisire il consenso al trattamento dei dati da parte dell'interessato, informandolo sulle finalità e le modalità del trattamento cui sono destinati i dati, i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza, la natura facoltativa o obbligatoria del conferimento dei dati e delle conseguenze del negato consenso, gli estremi identificativi del Titolare del trattamento, e di eventuali Responsabili, e i diritti di cui l'interessato dispone (articoli 13 e 7 del D. Lgs. 196/2003);
- implementa un'idonea procedura di gestione delle istanze dell'interessato, qualora questo decida di esercitare i diritti di cui all'art. 7 del Codice Privacy come la richiesta di aggiornamento, rettifica, integrazione, cancellazione, trasformazione dei dati in forma anonima o il blocco dei dati trattati in violazione di legge, ovvero l'opposizione per motivi legittimi al trattamento dei propri dati personali, ancorché pertinenti allo scopo della raccolta. A tal fine ASTEM S.p.A. deve agevolare l'accesso ai dati personali da parte dell'interessato, semplificare le modalità e ridurre i tempi per il riscontro al richiedente;
- predispone informative diverse in base alle diverse categorie di interessati destinatari delle stesse (informative diverse per Clienti, Fornitori, Dipendenti, Collaboratori/Professionisti, ecc.);
- archivia copia dell'informativa consegnata all'interessato e modulo di conferimento del consenso al trattamento dei dati acquisito in forma scritta;
- nomina formalmente per iscritto, sulla base della struttura aziendale, i c.d. "Responsabili esterni" - nel caso in cui dati acquisiti da ASTEM S.p.A. vengano trattati anche da terzi - impartendo a tal fine opportune ed idonee istruzioni. Una lista con indicazione dei Responsabili esterni è sempre accessibile da parte degli interessati e consultabile sul sito istituzionale della Società;
- nomina in forma scritta "Incaricati" per il trattamento tutti coloro che effettuano materialmente le operazioni di trattamento. Ogni persona fisica dipendente o collaboratore della Società deve essere incaricata per iscritto con la specificazione

delle modalità cui deve attenersi nel trattamento dei dati personali, anche in considerazione delle specifiche mansioni svolte;

- archivia copia controfirmata per accettazione delle nomine a “Responsabili” ed “Incaricati”;
- adotta idonee misure di sicurezza sia per gli archivi cartacei che per quelli elettronici, implementando un sistema di autenticazione informatica che consenta l’accesso solamente agli utenti dotati delle necessarie credenziali di autenticazione; una serie di requisiti per le credenziali di autenticazione; la presenza di un sistema di autorizzazione per l’assegnazione di diritti diversi agli utenti in funzione dell’attività svolta; la presenza di strumenti elettronici (firewall e antivirus), da aggiornare almeno semestralmente, che proteggano i dati personali dal rischio di intrusioni; l’aggiornamento di programmi (patch) per la prevenzione della vulnerabilità degli strumenti elettronici utilizzati (da aggiornare almeno annualmente o semestralmente nel caso di trattamento di dati sensibili); il salvataggio (backup) dei dati con cadenza almeno settimanale; la cifratura o separazione dei dati idonei a rilevare lo stato di salute dagli altri dati personali dell’interessato; la cifratura dei dati sensibili eventualmente trasferiti;
- verifica ogni anno l’elenco dei trattamenti svolti e gli strumenti utilizzati, la ripartizione di compiti e responsabilità derivanti dalla normativa sulla privacy, l’analisi dei rischi che incombono sui dati (e imputabili a comportamenti degli operatori, agli strumenti, al contesto fisico-ambientale), le modalità di ripristino dei dati in caso di distruzione o danneggiamento, la previsione di interventi formativi sul personale - al momento dell’assunzione, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, descrizione delle modalità di gestione dei dati affidati all’esterno, individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell’interessato;
- segnala con affissione di appositi cartelli la presenza all’interno della sede di eventuali aree sottoposte a videosorveglianza, avendo altresì cura di predisporre una informativa per i visitatori, specificando che eventuali immagini registrate sono conservate per motivi di sicurezza.

Solo il personale autorizzato può avere accesso a tali immagini, con specifiche indicazioni a riguardo contenute nella nomina ad “Incaricato”.

- (ii) ***Invio di newsletter;***
- (iii) ***Navigazione sul sito web aziendale;***
- (iv) ***Utilizzo e gestione della piattaforma E-Procurement;***
- (v) ***Utilizzo e gestione della piattaforma Whistleblowing;***
- (vi) ***Utilizzo e gestione degli altri software e piattaforma in uso all’azienda.***

Con particolare riferimento alla navigazione sul sito web aziendale, la società applica, in aggiunta a quanto già previsto al punto precedente i seguenti accorgimenti:

- la navigazione sul sito web aziendale avviene sempre previa possibilità all’utente di:
 - a) esame della informativa sul trattamento dati personali per la navigazione del sito;

- b) esame dell'informativa cookies;
- c) scelta tra il rifiuto e/o l'accettazione totale o selettiva della politica dei cookies adottata;
- non viene eseguita profilazione delle attività di navigazione sul sito web aziendale. Nel caso venisse avviata una attività di profilazione la stessa dovrà avvenire solo dietro consenso espresso dell'interessato;
- la cessione dei dati degli interessati avviene sempre nel rispetto di quanto previsto dalla normativa vigente e quindi, la cessione dei dati basata su obbligo di legge o contrattuale è sempre consentita per quei trattamenti le cui finalità ineriscono adempimenti di obblighi normativi o contrattuali, mentre la cessione dei dati per finalità di marketing dovrà essere basata su consenso dell'interessato;
- conseguentemente potranno essere inviate newsletter con finalità commerciali o di marketing unicamente agli interessati che abbiano manifestato consenso in tal senso;
- la società, per il tramite del responsabile IT Governance, tiene traccia dei consensi forniti e delle revoche dei consensi ricevute, provvedendo a escludere dall'invio delle newsletter gli interessati che abbiano revocato i consensi;
- ASTEM S.p.A. garantisce agli interessati, da parte del provider dello spazio web su cui sono caricati il proprio sito web, la piattaforma E-procurement e la piattaforma Whistleblowing, le stesse garanzie organizzative e tecnico-informatiche dalla stessa applicate in ottemperanza al dettato del D.lgs 196/2003 e del Regolamento UE 2016/679 GDPR.

7. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività di ASTEM S.p.A. potenzialmente a rischio di compimento dei Delitti informatici e di trattamento illecito di dati che sono stati inclusi nel piano di lavoro approvato dall'Organismo stesso, in funzione della valutazione del rischio assegnata in sede di predisposizione del Modello e nel corso dei suoi successivi aggiornamenti.

Tali controlli sono diretti a verificare la conformità dei comportamenti in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente alle fattispecie di attività sensibili.

Inoltre l'Organismo di Vigilanza esercita le proprie funzioni di controllo anche attraverso richiesta di specifici flussi informativi in materia di sicurezza informatica e trattamento dei dati.

A tal fine all'Organismo di Vigilanza deve essere trasmessa la relazione di Audit annuale redatta dal DPO Data Protection Officer (RPD – Responsabile della Protezione dei Dati) e ogni aggiornamento apportato al Progetto di Protezione dei Dati personali adottato da ASTEM S.p.A. (c.d. MOP - Modello organizzativo Privacy).

Può inoltre richiedere informazioni e specifiche relazioni a:

- Responsabile IT nominato;
- Responsabile Unico del Trattamento dei Dati Personali Interno (RDT).

L'Organismo di Vigilanza riferisce di detti controlli all'Organismo di Gestione.

8. DIFFUSIONE E FORMAZIONE

In relazione a tutto quanto sopra, ASTEM S.p.A. assicura ampia diffusione alle procedure stabilite nel presente Protocollo e nei documenti relativi e connessi ed un'adeguata formazione di base verso tutte le funzioni interessate in merito.

9. SANZIONI

La mancata osservanza delle procedure e dei principi a presidio delle attività aziendali e nel presente Protocollo è sanzionata secondo quanto previsto nel sistema disciplinare adottato da ASTEM S.p.A..