INDICE

Revisione	Descrizione modifica			Data
0	Prima emissione			23/10/2024
Redatto	Verificato (DPO)	Verificato (RESP. IT)	Verificato (AMM)	Approvato (CDA)
Roberto Redaelli	Veronica Devetag	Alessandro Asti	Simona Devecchi	23.10.2024

1. PREMESSA NORMATIVA

1.1. I reati in tema di strumenti informatici

La normativa italiana classifica l'uso dei computer e, in generale, degli strumenti informatici tra le attività pericolose ai sensi dell'articolo 2050 c.c. e questo comporta delle responsabilità specifiche sia per le persone che li utilizzano sia per le organizzazioni che ne sono proprietarie.
Anche dal punto di vista penale, l'attività svolta con i computer ha assunto una rilevanza particolare.
Di seguito si riportano i testi delle norme che descrivono le fattispecie di reato rilevanti in tema di utilizzo di strumenti informatici che comportano responsabilità penale per l'autore dell'illecito e responsabilità amministrativa per la società ai sensi 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:*** *ai 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".

*

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".

*

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]".

*

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".

*

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".*

*

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)".

*

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".

*

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.".

*

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)".
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*".

*

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*".

*

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*".

1.2. Il D.lgs 196/2003 così come modificato dal d.lgs. 101/2018 in attuazione del Regolamento UE 2016/679

1.2.1. Illeciti penali

Il d.lgs. 196/2003 prevedeva una serie di illeciti aventi rilevanza penale che è stato rivisto a seguito dell'emanazione del Regolamento UE 2016/679 (c.d. GDPR) e del d.lgs. 101/2018.

Attualmente le fattispecie penali in vigore sono essenzialmente dolose (dolo specifico) e sono le seguenti:

Art. 167 (Trattamento illecito di dati)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

*

Art. 167-bis (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.
3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

*

Art. 167-ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso
contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.
2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

*

Art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante)

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

*

Art. 170 (Inosservanza di provvedimenti del Garante)

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonché i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'articolo 13 della legge 25 ottobre 2017, n. 163 è punito con la reclusione da tre mesi a due anni.

*

Art. 171 (Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori)

1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.

1.2.2. Illeciti amministrativi

Il regolamento UE 2016/679 e il d.lgs. 101/2018 hanno al contrario rafforzato le fattispecie che prevedono violazioni amministrative.

Di esse si risponderà dunque a prescindere dalla volontà di commettere un illecito (dolo) e anche solo per colpa.

Il nuovo art. 166 del d.lgs. 196/2003 così come modificato dal d.lgs. 101/2018 prevede quanto segue:

Art. 166 (Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori)

1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-quinquies, comma 2, 2-quinquiesdecies, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-ter. Alla medesima sanzione amministrativa è soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.
2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 8, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonché delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.
3. Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attività di cui al comma 4 configurino una o più violazioni indicate nel presente titolo e nell'articolo 83, paragrafi 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare.

6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 3 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento svolte dal Garante.

8. Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

9. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformità ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonché della distinzione tra
funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.

10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.

L'art. 82 del GDPR, stabilisce che:

a) Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
b) Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
c) Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
d) Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
e) Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Fermo quanto sopra in tema di risarcimento del danno, l'art. 83 prevede che ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte siano in ogni singolo caso effettive, proporzionate e dissuasive.

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

Tabella delle sanzioni

violazione	sanzione
gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43	sanzioni amministrative pecuniarie fino a 10.000.000,00 di euro, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43	
gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;	
principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9	sanzioni amministrative pecuniarie fino a 20.000.000,00 di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore
diritti degli interessati a norma degli articoli da 12 a 22	
trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;	
qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX	
l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1	

l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2	

Ogni dipendente/collaboratore di ASTEM S.p.A. deve prendere buona nota del contenuto delle disposizioni di legge sopra richiamate, impegnandosi a non violarle e a non costituire situazioni di rischio di violazione.

Ogni violazione e ogni comportamento che possa recare rischio di violazione verrà sanzionato nel rispetto della normativa regolante il rapporto di lavoro/collaborazione.

2. FINALITA' DEL PRESENTE DOCUMENTO

L'utilizzo di strumenti elettronici e cartacei per il trattamento dei dati forniti a ASTEM S.p.A. dai suoi interlocutori, siano essi clienti, fornitori, collaboratori, dipendenti o altro, è inoltre vincolato al rispetto delle normative in essere (legali, fiscali, amministrative, eccetera), compresa quella sulla tutela dei dati personali. In aggiunta è fondamentale che gli strumenti e le risorse di ASTEM S.p.A. siano finalizzati al mantenimento, nel tempo, di un adeguato livello di sicurezza per la conservazione e la protezione dei dati.

Per tali ragioni nel presente documento sono indicate le regole di comportamento interne adottate da ASTEM S.p.A. volte a salvaguardare sia gli utenti sia ASTEM S.p.A. dalla possibilità che possano verificarsi nell'ambito dell'attività professionale fatti illeciti e/o pericolosi nelle operazioni di trattamento di dati per mezzo di strumenti elettronici.

Il presente documento descrive le politiche generali di sicurezza che ASTEM S.p.A. ha deciso di adottare in tema di utilizzo di posta elettronica e internet sulla base delle Linee Guida del garante e della prassi instauratesi nella vigenza del d.lgs. 196/2003.

Il presente documento viene redatto dall'Organo Amministrativo ed è soggetto ad aggiornamento periodico coerentemente con l'aggiornamento del Progetto di Protezione dei Dati Personali nonché all'esposizione tramite intranet, e-mail e/o consegna cartacea ai dipendenti.

Ogni dipendente e collaboratore di ASTEM S.p.A. è tenuto a prenderne atto, osservarne i contenuti ed a conformarvi il proprio comportamento. **Qualsiasi comportamento che disattenda quanto ivi contenuto sarà sanzionabile disciplinarmente**.

3. REGOLE GENERALI

Le regole descritte nel presente documento hanno valenza generale e vanno quindi applicate indipendentemente dallo strumento e/o dai dati presi in considerazione.

3.1. Trattamento dei dati

Per quanto riguarda il trattamento dei dati occorre che l'incaricato/utente per quanto possibile:

- eviti di trattare particolari categorie di dati ex art. 9 GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, ossia gli ex "dati sensibili") o dati giudiziari fatto salvo che l'utente stesso svolga mansioni che ne richiedano l'utilizzo oppure nei casi di comprovata necessità.
- informi tempestivamente un amministratore e/o il Responsabile Unico per il Trattamento dei Dati interno (RDT) e/o il Responsabile per la Protezione dei Dati (DPO) qualora l'utente stesso riceva o entri in possesso o diffonda erroneamente informazioni (tramite, ad esempio, posta elettronica o supporto magnetico) di competenza non sua e/o del reparto di appartenenza;
- possa dimostrare in ogni momento di aver agito con la massima diligenza e con tutti i mezzi a sua disposizione al fine di preservare la sicurezza del patrimonio dati aziendale, attenendosi scrupolosamente alle disposizioni ricevute dagli amministratori.

4. DEFINIZIONI

4.1. Incaricato al trattamento/Utente

Per utente si intende una persona fisica addetta, a qualsiasi titolo, al trattamento di dati aziendali e, nella pratica, si intendono tutti i dipendenti ed i collaboratori di ASTEM S.p.A.

4.2. Trattamento

Si intende 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.

4.3. Responsabile del trattamento

Si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

4.4. Titolare del trattamento

Si intende 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, ivi compreso il profilo della sicurezza, nello specifico ASTEM S.p.A..

4.5. PDL

Si definisce postazione di lavoro (in seguito PDL) una locazione stabile o mobile dalla quale l'incaricato è in grado di interagire con il sistema informativo aziendale in maniera diretta o indiretta.
Per accesso in via indiretta al sistema informativo aziendale si intende la possibilità per l'incaricato di operare su dati memorizzati su apparecchiature fornite insieme alla PDL aziendale, anche in mancanza di un collegamento diretto. La PDL è normalmente composta da un personal computer (PC) da tavolo (desktop) o portatile (laptop) e può essere costituita da altri strumenti idonei al trattamento dei dati come per esempio:

- Stampante (anche se in rete e condivisa);
- Tablet;
- smartphone.

Non a tutti gli incaricati viene assegnata la strumentistica sopra riportata.

4.6. Dati

Si intendono per dati, tutte le tipologie utilizzate all'interno dell'azienda sia attraverso strumenti elettronici che cartacei. Per maggiori dettagli ci si riferisca al materiale in materia di trattamento dei dati, fornito in sede di assunzione/formazione.
Fanno parte dei dati di pertinenza dell'azienda anche quelli relativi alla struttura organizzativa dell'azienda stessa ed alla configurazione Hardware (HW) e Software (SW) degli strumenti che compongono il sistema informativo dell'azienda (computer, stampanti, programmi, user-id, password, etc.) e degli impianti di ricerca e sviluppo e produzione.

4.7. Incaricato

Per incaricato si intende qualsiasi dipendente e/o collaboratore e/o consulente esterno che acceda ad una PDL per via delle mansioni attribuite e/o degli incarichi affidati. Questo ha valore quindi anche per i collaboratori e/o consulenti esterni che accedono a PDL messe a disposizione dall'azienda.

4.8. Amministratore di Sistema

L'Amministratore di Sistema è colui che si occupa della gestione, dell'amministrazione e della manutenzione di sistemi informatici all'interno di un'azienda.
L'Amministratore di Sistema è la figura dedicata alla gestione ed alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (*enterprise resource planning*), le reti locali, i server, i siti e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.
In particolare, quindi, con l'espressione amministratore di sistema possono individuarsi una pluralità di figure con ruoli e responsabilità ben definite:

- amministratore di sistema: personale addetto alla gestione dei sistemi, sia a livello hardware, sia a livello software (sistema operativo e applicazioni);
- amministratore di rete: personale addetto alla manutenzione, configurazione ed aggiornamento delle componenti di rete (router, switch), nonché alla struttura stessa della rete:
- amministratore di database: personale addetto alla gestione delle base dati aziendali;
- amministratore di sicurezza: personale addetto alla gestione di utenze, ruoli e profili d'accesso; è responsabile di assicurare l'installazione, la configurazione, l'amministrazione e la risoluzione dei problemi legati agli apparati di sicurezza;
- amministratore di software complessi: figura professionale responsabile di assicurare l'installazione, la configurazione, l'amministrazione e la risoluzione dei problemi legati ai sistemi software complessi (e.g. SAP, sistemi CRM).

L'Amministratore di Sistema può gestire l'infrastruttura informatica di una azienda nel suo complesso, oppure singole banche dati come ad esempio un sito web, un social network, il server utilizzato ai fini di backup.
Le principali mansioni attribuite all'Amministratore di Sistema vi sono:

- Installazione e configurazione dei sistemi operativi: l'amministratore di sistema è responsabile dell'installazione e della configurazione dei sistemi operativi sui server e sulle workstation dell'azienda. Deve assicurarsi che i sistemi siano correttamente configurati e ottimizzati per le esigenze dell'azienda.
- Gestione delle reti: l'amministratore di sistema si occupa della gestione e della configurazione delle reti aziendali, compresi i router, gli switch e i firewall. Deve garantire la sicurezza e la stabilità delle reti, nonché l'accesso corretto alle risorse condivise.
- Amministrazione dei server: l'amministratore di sistema è responsabile della gestione dei server aziendali, inclusi i server di posta elettronica, i server web, i server di database e altri server specifici per le esigenze dell'azienda. Deve assicurarsi che i server siano sempre disponibili, sicuri e performanti.
- Gestione degli account utente: l'amministratore di sistema si occupa della gestione degli account utente all'interno dell'azienda. Deve creare, modificare e disabilitare gli account utente in base alle esigenze dell'azienda, garantendo al contempo la sicurezza e l'accesso corretto alle risorse aziendali.
- Backup e ripristino dei dati: l'amministratore di sistema deve pianificare e gestire i backup dei dati aziendali, assicurandosi che i dati siano protetti da perdite o danni. In caso di incidenti o guasti, deve essere in grado di ripristinare i dati in modo tempestivo.

4.9. Responsabile per la Protezione dei Dati personali (RPD) o Data Protection Officer (DPO)

È la figura che affianca il titolare e/o il responsabile del trattamento per le funzioni di supporto, controllo e prassi formative e informative sulle disposizioni normative in tema dio trattamento dati personali.
Ai sensi dell'art. 39 del Regolamento UE 2016/679 il responsabile della protezione dei dati è incaricato dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il DPO è raggiungibile alla seguente casella e-mail dpo@astemlodi.it

4.10. Responsabile Unico del Trattamento dei Dati Personali Interno (RDT)

È il referente interno in materia di trattamento dati personali.
Il RDT è raggiungibile alla seguente casella e-mail p_bottajoli@hotmail.com

5. DISPOSIZIONI SPECIFICHE

Le seguenti disposizioni hanno valenza generale e vanno quindi applicate indipendentemente dallo strumento e/o dal trattamento dei dati preso in considerazione.

5.1. Uso delle apparecchiature

Sono da applicarsi le seguenti regole:

- fatta eccezione per eventuali situazioni contingenti, dietro autorizzazione del responsabile di settore e del responsabile IT, in nessun caso l'incaricato dovrà utilizzare per il trattamento dei dati aziendali, apparecchiature diverse da quelle di proprietà dell'azienda e fornite all'incaricato stesso al fine di adempiere alle mansioni affidategli;
- l'incaricato è tenuto a utilizzare gli strumenti informatici che l'azienda mette a sua disposizione solo per il trattamento di dati, documenti, files, programmi con finalità attinenti alle mansioni affidategli all'interno dell'azienda;
- non sono quindi consentiti il trattamento (inteso come creazione, modifica, salvataggio, consultazione, ecc.), la trasmissione e/o la stampa di materiale che abbia contenuti non connessi con l'attività dell'azienda ed in ogni caso, qualsiasi informazione che possa ricadere in qualcuna delle seguenti categorie che vengono riportate a titolo esemplificativo ma non esaustivo:
    - materiale che abbia riferimenti o attinenze con l'aspetto politico e/o religioso;
    - materiale che sia riconducibile ad attività di tipo personale condotte a qualsiasi titolo, anche a non a scopo di lucro;
    - materiale ludico e/o di intrattenimento (giochi, utilities, sfondi colorati, fotografie, immagini, ecc.) non riconducibile all'attività svolta dall'incaricato con riferimento alle mansioni affidategli;
    - materiale con contenuti contrari al comune senso del pudore, pornografia, pedofilia, ecc.;
    - materiale soggetto alla legislazione nazionale ed internazionale sul diritto d'autore, sulla proprietà intellettuale, sui brevetti, ecc.
- è fatto divieto di utilizzare gli strumenti forniti dall'azienda per mostrare e/o trasmettere, all'esterno dell'azienda, dati sensibili ai fini privacy e/o riservati con riferimento alle attività e alla strategia aziendali;
- è fatto divieto utilizzare PC o strumenti non autorizzati dall'azienda per il trattamento dei dati;
- è fatto divieto di accedere senza autorizzazione a sistemi informatici di terzi. Nel caso in cui ciò fosse necessario per finalità aziendali, l'incaricato dovrà richiedere autorizzazione al proprio responsabile e seguire le misure di sicurezza dallo stesso indicate per eseguire l'accesso.

5.2. Divieto di uso di PDA Personali / Smartphone

Non è consentito l'uso di notebook e Smartphone non di proprietà dell'azienda per il trattamento di dati della struttura. In nessun caso l'utente potrà memorizzare, su dispositivi non di proprietà dell'azienda, dati relativi all'attività dell'azienda stessa anche attraverso lo scambio via protocolli wireless come Bluetooth o similari.

5.3. Internet

È fatto divieto agli incaricati al trattamento di utilizzare PdL forniti dall'azienda per:

- navigare in siti non attinenti allo svolgimento delle proprie mansioni;
- navigare su siti che presentino contenuti a sfondo sessuale, pornografico e pedopornografico,

- partecipare, per motivi non professionali e non attinenti allo svolgimento delle proprie mansioni a forum, chat-line, trading on-line, blog, sondaggi, ecc.;
- svolgere attività che influenzino negativamente la regolare operatività della rete dell'azienda o ne alterino l'utilizzabilità;
- l'utilizzo di sistemi di comunicazione diversi da quelli forniti dall'IT dell'azienda; questo vale sia per i collegamenti verso l'esterno, sia per i servizi di messaggistica immediata (Skype, Whatsapp, MSN Messenger, AOL Messenger, ICQ o similari), in quanto sono potenziali veicoli di intrusione o di diffusione di informazioni riservate. È consentito l'utilizzo di Whatsapp Business per motivi di lavoro e sui soli device aziendali. Qualora altro servizio di messaggistica immediata dovesse essere ritenuto utile dal punto di vista dell'azienda, verrà fornito uno strumento apposito, gestito dall'IT dell'azienda.
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- scaricare files, anche su supporti magnetici/ottici, non aventi alcuna attinenza con le mansioni assegnate;
- utilizzare programmi e/o files audio o video non consoni con le mansioni ed i compiti assegnati;
- effettuare il download da Internet di materiale protetto da copyright o dalla legge sul diritto d'autore; qualora sulla rete aziendale o sui dischi fissi locali dei singoli PC / Pdl vengano individuati file di questo tipo si procederà d'ufficio alla loro rimozione;
- redigere, copiare, memorizzare, trasmettere documenti informatici di natura discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica o di natura oltraggiosa, diffamatorio, oscena, ingiuriosa o altrimenti offensiva o illecita;
- Accedere a siti di social network come per esempio www.facebook.com, www.instagram.com, www.live.it, www.twitter.com, ecc. se non necessario per esigenze lavorative (ad es. rintracciare recapiti o assumere informazioni su un cliente o su un fornitore);

Le suddette disposizioni si applicano alla navigazione Internet sia che venga effettuata tramite computer desktop o laptop piuttosto che attraverso Smartphone di proprietà dell'azienda e/o messi a disposizione degli incaricati dell'azienda.

È facoltà dell'azienda esercitare controlli per la verifica del corretto adempimento di quanto sopra disposto.

6. REGOLAMENTO PER IL CORRETTO UTILIZZO DEGLI STRUMENTI ELETTRONICI

6.1. Accesso alla PdL

Per accedere alle informazioni ed ai servizi del sistema informativo, l'incaricato deve fornire le proprie credenziali di accesso (user id e password) e provvedere all'esecuzione della procedura di accesso (log on). È fatto obbligo di disconnettersi (log off) al termine dell'orario di lavoro e di bloccare la PdL (vedi in seguito) in caso di assenze anche brevi.

Le credenziali di accesso alla PdL sono fornite all'incaricato dalla funzione IT e sono da considerarsi informazioni riservate e da trattarsi conseguentemente con le necessarie cautele.

L'incaricato è tenuto a seguire in tema di password le regole indicate al successivo paragrafo 6.4.

- alla prima assegnazione, l'incaricato - non appena effettuata l'autenticazione - dovrà provvedere a sostituire la password con una che risponda ai requisiti di sicurezza a 4 fattori (password alfanumerica con utilizzo di caratteri maiuscoli, minuscoli, numeri e caratteri speciali, che non deve contenere più di due caratteri identici consecutivi);
- la password non deve contenere riferimenti agevolmente riconducibili all'incaricato (es.: cognome, nome, codice di accesso, user id, data di nascita, riferimenti facilmente riconducibili a familiari, ecc.),
- la password non deve essere simile alla password precedente;
- la password non deve essere comunicata ad altri utenti;
- la password deve essere sostituita ogni 3 mesi ovvero con la diversa frequenza prevista dalle politiche di sicurezza dell'azienda;
- in caso si richieda il ripristino della password, per diverse motivazioni, l'utente dovrà cambiarla subito dopo.

La password è personale ed è strettamente riservata. Conseguentemente non deve essere divulgata ad alcuno (ivi compresi personale interno e/o esterno ovvero terzi). Nel caso l'incaricato abbia anche solo il sospetto che altri incaricati ne siano venuti a conoscenza, dovrà attivarsi per cambiarla avvisando la funzione IT del possibile rischio di intrusione non autorizzata.

Le password sono custodite dall'incaricato stesso con l'adozione di misure di sicurezza (se in cartaceo, in busta chiusa riposta in armadio chiuso a chiave; se in digitale su file protetto da crittografia).

Il Gestore IT può, su richiesta dell'interessato ovvero dell'amministrazione, resettare la password.

6.2. Blocco temporaneo della PdL

Dopo un predeterminato periodo di inattività (massimo 10 minuti) la Pdl provvede automaticamente ad entrare in uno stato di blocco dal quale può essere fatta uscire solo dall'incaricato attraverso la digitazione delle proprie credenziali di accesso (user id e password).

6.3. Utilizzo della PdL

L'incaricato dovrà agire con la massima diligenza e con tutti i mezzi a sua disposizione al fine di preservare la sicurezza del patrimonio dati dell'azienda.

L'incaricato dovrà farsi carico di ridurre il dispendio di risorse (carta, toner, fotocopie, ecc.) dovuto a incorretto utilizzo delle apparecchiature. Per esempio, dovrà evitare di:

- stampare documenti non necessari;
- utilizzare applicazioni grafiche se non necessario;
- utilizzare internet se non necessario;

- spedire allegati di grandi dimensioni;
- utilizzare risorse aziendali per fini personali.

È espressamente vietato all'incaricato di intervenire sulla PdI modificando la configurazione della stessa (software e/o hardware).

È in particolar modo vietato scaricare autonomamente programmi software senza l'autorizzazione del proprio responsabile della funzione IT.

Ogni intervento di modifica dovrà essere richiesto al proprio responsabile diretto che interesserà la funzione IT, la quale – se del caso - provvederà a realizzarlo qualora necessario e in accordo con gli standard dell'azienda.

6.4. Password

L'incaricato è tenuto a seguire in tema di password le seguenti regole.

- alla prima assegnazione, l'incaricato - non appena effettuata l'autenticazione - dovrà provvedere a sostituire la password con una che risponda ai requisiti di sicurezza a 4 fattori (password alfanumerica con utilizzo di caratteri maiuscoli, minuscoli, numeri e caratteri speciali, che non deve contenere più di due caratteri identici consecutivi);
- la password non deve contenere riferimenti agevolmente riconducibili all'incaricato (es.: cognome, nome, codice di accesso, user id, data di nascita, riferimenti facilmente riconducibili a familiari, ecc.),
- la password non deve essere simile alla password precedente;
- la password non deve essere comunicata ad altri utenti;
- la password deve essere sostituita ogni 3 mesi ovvero con la diversa frequenza prevista dalle politiche di sicurezza dell'azienda;
- in caso si richieda il ripristino della password, per diverse motivazioni, l'utente dovrà cambiarla subito dopo.

La password è personale ed è strettamente riservata. Conseguentemente non deve essere divulgata ad alcuno (ivi compresi personale interno e/o esterno ovvero terzi). Nel caso l'incaricato abbia anche solo il sospetto che altri incaricati ne siano venuti a conoscenza, dovrà attivarsi per cambiarla avvisando la funzione IT del possibile rischio di intrusione non autorizzata.

È vietato:

- scrivere la password su taccuini o foglietti;
- utilizzare le stesse credenziali di accesso al sistema informativo dell'azienda, ed in particolare la password, per l'accesso a servizi esterni, anche se utilizzati per ragioni lavorative.

Le password sono custodite dall'incaricato stesso con l'adozione di misure di sicurezza (se in cartaceo, in busta chiusa riposta in armadio chiuso a chiave; se in digitale su file protetto da crittografia).

Il Gestore IT può, su richiesta dell'interessato ovvero dell'amministrazione, resettare la password.

6.5. Posta elettronica

Il sistema di posta elettronica (e-mail) dell'azienda è un servizio che permette agli utenti del sistema informativo di scambiarsi messaggi e allegati. Per allegati si intende qualsiasi file che può essere prodotto con uno dei software presenti nella dotazione standard della PdI aziendale. In funzione delle mansioni ricoperte in azienda, vengono assegnate ai vari incaricati delle caselle postali dell'azienda.

L'utilizzo a fini personali della casella di posta elettronica dell'azienda è assolutamente vietato.

Analogamente l'utilizzo della posta elettronica su smartphone è da utilizzarsi solo a fini professionali.

6.6. Gestione della casella postale

La casella postale dell'incaricato è personale e deve essere accessibile solo fornendo le credenziali dello stesso. Per nessuna ragione la casella postale deve essere utilizzata da un incaricato diverso, salvo esplicita richiesta dello stesso di delegare l'accesso a personale di segreteria ovvero per necessità professionali o che per particolari esigenze gestionali rendano necessario ed urgente l'accesso da parte di altri incaricati ovvero in caso di assenza prolungata dello stesso incaricato assegnatario.

Le deleghe di accesso alla casella postale vanno richieste mediante notifica e-mail al proprio responsabile che, a sua volta, provvederà ad autorizzare la funzione IT.

Poiché potrebbero rendersi necessari detti accessi in assenza dell'assegnatario della casella di posta elettronica, accessi giustificati e legittimi alla luce del fatto che detta casella è un bene dell'azienda strumentale, messo a disposizione al singolo incaricato, dall'azienda in accordo con le funzioni assegnate allo stesso, l'azienda non potrà in nessun caso ritenersi responsabile qualora, in tale frangente, dovessero divenire pubbliche informazioni riservate e personali inerenti l'incaricato stesso.

È fatto divieto di utilizzare l'indirizzo e-mail aziendale assegnato all'incaricato per creare account personali su app, siti web, social network e altre piattaforme.

L'incaricato è tenuto a salvare nelle apposite cartelle di rete le e-mail inviate o ricevute rilevanti per contenuto (ad es. e-mail rilevanti per la dimostrazione dell'adempimento di una prestazione, del contenuto contrattuale, di richieste da parte di clienti e fornitori, di contestazioni fatte o ricevute ed ogni altra comunicazione rilevante per le posizioni seguite dall'incaricato).

<u>Comportamenti da osservare:</u>

- In caso di assenza l'utente dovrà utilizzare la funzione "Fuori Sede" o "Out of Office". In caso di assenza prolungata (malattia, maternità, ferie, ecc.) inserire nel messaggio che notifica il "Fuori Sede", il nominativo e i recapiti dei colleghi cui i mittenti possono rivolgersi per avere pronta risposta. Esempio: "*Sono momentaneamente assente. La Vs. e-mail verrà presa in considerazione al mio rientro. In caso di urgenza contattare XXXXXXXX (e-mail: XXXXXXXXX)*".
- In fondo al messaggio di posta aggiungere sempre, in accordo con le disposizioni aziendali in materia, i dati come indicato nell'esempio seguente:
    - Nome e Cognome, Job Title, Indirizzo, Città, Telefono, Cellulare aziendale (se assegnato), Indirizzo e-mail
- Non comunicare a terzi – se non a ciò espressamente autorizzati - informazioni riguardanti l'azienda.
- Per ogni comunicazione cercare di utilizzare un singolo messaggio per raggiungere tutti i destinatari interessati. Allo stesso tempo però è consigliabile spedire messaggi a non più di una decina di destinatari alla volta.
- Assicurarsi di utilizzare la funzione "*non-disclosure-recipient*" (o CCN – Copia Conoscenza Nascosta) per gli invii a un numero rilevante di destinatari.
- La funzione "*inoltra messaggio*" altrui va utilizzata verso altri destinatari solo mettendo in copia conoscenza (cc) il mittente originale.
- Non spedire allegati superiori a 10 MB se non strettamente necessario. In caso di necessità di invio di file di dimensione superiore, ove possibile, suddividere gli allegati in più messaggi di posta. Ove ciò non sia possibile utilizzare, previa autorizzazione del proprio responsabile e della funzione IT, il programma Onedrive di Microsoft 365.

- Utilizzare la funzione copia per conoscenza (cc) solo se necessario e coinvolgendo solo i destinatari realmente interessati.
- Nell'oggetto della e-mail essere sintetici in modo che il destinatario capisca subito cosa fare del messaggio.
- Nell'oggetto della e-mail evitare di fare riferimento a persone.
- Utilizzare gli allegati solo se strettamente necessario.
- Nel caso di allegati di grandi dimensioni, utilizzare i programmi di compressione messi a disposizione dalla funzione IT per ridurli.
- In caso di ricezione di un file di tipo eseguibile (.exe) non aprirlo senza prima aver consultato la funzione IT.

Comportamenti vietati:

- Rispondere alle "catene di S. Antonio".
- Utilizzare la posta elettronica per esprimere punti di vista ufficiali dell'azienda a meno che si sia stati a ciò espressamente autorizzati.
- Utilizzare la posta elettronica per spedire informazioni riservate (listini, prezzi, statistiche, dati di mercato, struttura organizzativa dell'azienda, ecc.) salvo nei casi previsti. Se dette informazioni devono essere inviate verso l'esterno, è opportuno ottenere la preventiva autorizzazione del Titolare.

Comportamenti sconsigliati:

- Cancellare i messaggi prima ancora di averli letti, salvo che la provenienza sia dubbia. In questo caso, per evitare il contagio da possibili virus, cancellare l'e-mail.
- Aprire messaggi che provengono da mittenti sconosciuti e/o aventi contenuti dubbi o discutibili.
- Abusare delle funzionalità che qualificano un messaggio come urgente, se non per reali necessità.
- Abusare delle funzionalità di ricevuta di ritorno e ricevuta di avvenuta lettura se non necessario: si consumano risorse dei server centrali e della rete locale dell'azienda.

Alla cessazione del rapporto di lavoro:

- l'incaricato è tenuto a restituire al Titolare tutti gli strumenti elettronici consegnati per l'espletamento delle prestazioni di lavoro senza cancellare alcun dato;
- la casella di posta elettronica e l'account dell'incaricato saranno immediatamente disattivati e inibiti alla ricezione dei messaggi. Non verranno applicati funzioni di *redirect* ad altre caselle. Il mittente dovrà ricevere idoneo avviso che informi che la casella destinataria non è più attiva e che indichi la nuova casella a cui indirizzare i messaggi.

6.7. Rubrica Personale

È vietato utilizzare la rubrica del sistema di posta elettronica dell'azienda per memorizzare indirizzi di posta personali.

6.8. Utilizzo di software e piattaforme aziendali

I programmi e le piattaforme in uso all'azienda (ad es. Gestionale GO, Software DiMasi, Software Costner, Software PA Digitale, E-Procurement Traspare, ecc.) possono essere utilizzati solo dagli incaricati a ciò espressamente autorizzati.

Ognuno degli incaricati deve accedere con proprio account personale.

Gli account in uso agli incaricati non devono essere utilizzati o rivelati ad altri dipendenti o a terzi.

La piattaforma Whistleblowing è in uso, lato gestore, al RPCT. Lato segnalatore può essere utilizzata da tutti gli incaricati secondo la procedura approvata e pubblicata sul sito web.

6.9. Utilizzo di programmi per videoconferenze

In caso di necessità di partecipazione a videoconferenze gli incaricati dovranno utilizzare gli account Microsoft Teams.

L'incaricato non potrà dare consenso alla registrazione della videoriunione, se non a ciò espressamente autorizzato dal proprio responsabile.

È vietato utilizzare altri software per videoconferenze (Skype, Zoom, Google Meet o similari).

6.10. Utilizzo di supporti magnetici

Oggetti rimuovibili atti alla memorizzazione dei dati di uso corrente sono: dischetti, nastri, CD, memorie USB hard disk portatili ed altro.

È vietato scaricare dati di qualunque natura e con qualunque finalità (personale o lavorativa) su supporti rimovibili, se non dietro autorizzazione del proprio responsabile e della funzione IT.

Non è comunque mai consentito l'utilizzo di memorie usb, cd rom, cd riscrivibili, nastri magnetici o altri dispositivi di provenienza ignota.

I supporti rimovibili contenenti dati personali o aziendali, se non utilizzati, devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se - mediante adeguata formattazione - le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Eventuali supporti rimovibili contenenti dati sensibili devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in archivi (armadio/cassetto) chiusi a chiave.

Tutti i files di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione all'utilizzo da parte dell'Amministratore del Sistema.

7. MISURE DI SICUREZZA

L'azienda ha la responsabilità di proteggere il proprio patrimonio dati e tutelarsi da comportamenti lesivi e/o dannosi.
Ai fini del mantenimento del suddetto livello di sicurezza sono intraprese alcune specifiche attività di controllo e monitoraggio qui di seguito elencate.

7.1. Internet

Sono applicate le seguenti misure di sicurezza e controllo:

- L'azienda si riserva la facoltà di oscurare o impedire l'accesso ai siti che possono compromettere la sicurezza delle connessioni e dei servizi che risultano in violazione della legislazione italiana e comunitaria vigente;
- al fine di garantire adeguata sicurezza al patrimonio dei dati dell'azienda, e anche al fine di ovviare alle situazioni di pericolo e/o rischio derivanti da attacchi ai sistemi informativi, tutti gli accessi ad Internet sono soggetti a monitoraggio da parte del Titolare. Gli accessi sono memorizzati in archivi elettronici che risultano essere:
    - soggetti a cancellazione periodica automatica da parte del software di controllo con cadenza trimestrale;
    - non accessibili al personale interno della LAN dell'azienda;
    - disponibili alle autorità competenti (Guardia di Finanza, Polizia, Carabinieri, Autorità Giudiziaria, Ispettori del Garante, ecc.) in caso di indagini e/o richieste specifiche.

7.2. Posta elettronica

- La casella postale dell'azienda viene eliminata all'atto della cessazione del rapporto tra dipendente o collaboratore e azienda (vedi procedura nel paragrafo seguente).
- Il sistema di posta elettronica dell'azienda viene protetto da sistemi automatici di controllo che provvedono a rifiutare messaggi di posta elettronica provenienti da siti ritenuti, dal sistema di controllo, dubbi e/o considerati generatori di mail inutili e/o dannose (spam).
- Il blocco viene attivato automaticamente su tutte le caselle postali dell'azienda ed è operativo a partire dalle segnalazioni provenienti dai sistemi di controllo internazionali fornite dai vari provider Internet.
- Nel caso l'incaricato sospetti che un messaggio di posta elettronica a lui inviato non sia stato ricevuto, deve provvedere ad avvisare il Titolare indicando l'indirizzo di posta elettronica completo del mittente.
- Le caselle postali "di funzione" possono essere rese disponibili, per necessità organizzative, a più incaricati di operare sulla stessa casella postale. La casella postale di funzione possiede quindi un indirizzo di posta elettronica che ne esemplifica al mittente la funzionalità (es.: amministrazione@astemlodi.it).

7.3. Utilizzo di archivi cartacei contenenti dati personali e particolari categoria di dati (ex dati sensibili)

Specifiche istruzioni sono fornite agli incaricati della Direzione del Personale per garantire adeguata sicurezza di trattamento dei dati sensibili del personale dipendente.
In particolare, per quanto riguarda i supporti cartacei:

- i curricula di potenziali candidati, per qualsiasi ruolo, devono essere conservati nell'ufficio amministrazione, in un armadio chiuso a chiave. In caso di curricula utilizzati all'esterno dell'ufficio precedentemente indicato questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo. I curricula devono

essere eliminati, una volta esaurita la procedura di selezione e se scaduti tutti i termini di contestazione o impugnazione. I curricula pervenuti alla Società, se non a corredo di una domanda di partecipazione a una selezione indetta secondo le procedure aziendali, devono essere immediatamente eliminati.

- i dati cartacei relativi alle presenze dei dipendenti devono essere conservati all'interno dell'ufficio amministrazione, in un armadio chiuso a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato, questi devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati cartacei relativi ai cedolini paga, alle malattie e in generale alle informazioni necessarie per la gestione delle retribuzioni e dei rapporti di lavoro devono essere conservati all'interno dell'ufficio amministrazione, in appositi archivi siti in armadi chiusi a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati e la documentazione relativi agli adempimenti di cui al D.Lgs. 81/2008 sono conservati nell'ufficio amministrazione, in un apposito archivio conservato in un armadio chiuso a chiave. In caso di utilizzo dei documenti all'esterno dell'ufficio precedentemente indicato, questi documenti devono essere riposti nel luogo prescritto subito dopo il loro utilizzo.
- i dati cartacei relativi a clienti e fornitori devono essere conservati all'interno dell'ufficio amministrazione, dell'ufficio commerciale e dell'ufficio magazzino in appositi archivi conservati in armadi chiusi a chiave. In caso di utilizzo dei documenti all'esterno degli uffici precedentemente indicati questi documenti devono essere riposti nei luoghi prescritti subito dopo il loro utilizzo.
- ogni volta che le persone incaricate del trattamento dei dati lasciano gli uffici della Società devono chiudere la porta a chiave, dopo aver riposto i documenti negli appositi cassetti/armadi.
- ogni volta che si raccolgono dati personali è necessario rilasciare l'informativa del caso all'interessato.
- non comunicare dati a persone non autorizzate.

7.4. Politica di *clean desk*

Le informazioni utilizzate per lo svolgimento delle proprie attività non devono essere visibili a persone non autorizzate. Pertanto, è necessario attenersi alle seguenti indicazioni:

- evitare di lasciare documenti sulla scrivania o in altri luoghi operativi in propria assenza;
- non permettere a persone non autorizzate al trattamento dati di accedere ai locali aziendali;
- archiviare tutti i documenti in modo sicuro come da politica di classificazione delle informazioni.

7.5. Politica di *clean screen*

Analogamente alla politica di Clear Desk si deve evitare di lasciare incustodite informazioni sulla propria stazione di lavoro, a tale fine devono essere attuate le seguenti condizioni:

- bloccare lo schermo prima di assentarsi;
- disporre di un sistema di blocco schermo automatico che si attivi dopo 10 minuti di inattività e che richieda l'accesso tramite credenziali;
- salvare prima di assentarsi ogni documento e/o cartella e/o file di lavoro nella pertinente partizione su server e non in locale sul proprio pc locale.

8. GESTIONE DELLA PROBLEMATICHE E DELLE EMERGENZE

8.1. Assistenza IT

La segnalazione di problemi tecnici o anomalie che impediscono il regolare svolgimento delle attività, deve essere effettuata al gestore IT nominato.

L'accesso alla PdL per attività di help desk è ammesso previo consenso dell'incaricato e preavviso. Il personale IT della società esterna è stato espressamente nominato ed autorizzato ad eseguire le suddette attività.

Le procedure di Help desk sono le seguenti:

Help Desk Q.Service S.r.l.:

Per le seguenti problematiche:

- Problemi hardware e software delle postazioni client;
- Problemi di login alle postazioni (password scadute, password non accettate, ecc..);
- Problemi sui server cloud (server documentale, server gestione calore…);
- Problemi di connessione di rete e connessione wireless;
- Problemi di stampa;

è possibile segnalare le problematiche tecniche e le anomalie contattando direttamente il personale di Q.Service Srl mediante mail o telefono.

Personale nominato:

ALESSANDRO ASTI alessandro.asti@q-service.it Cell. 3493728177

MARCO SOLA marco.sola@q-service.it Cell. 3493728069

Help Desk XStream S.r.l.:

Per problematiche di:

- Connessione internet (se l'evento si verifica da tutte le postazioni);
- Connessione ai server cloud (documentale e software gestionali – se l'evento si verifica da tutte le postazioni);
- Problematiche al sistema centralino/telefoni;
- Problematiche connessione internet dal magazzino;

è possibile procedere con le seguenti modalità:

Numero Verde: 800969787 (interno 3) del lunedi al venerdì , ore 8.30 – 18.00

Email: support@x-stream.biz

Portale assistenza: https://myportal.x-stream.biz (con le credenziali inviate da XStream Srl)

Non sono previste attività per il salvataggio dei dati contenuti sulle Pdl (drive locali quali C:\) e desktop. È responsabilità dell'utente memorizzare i dati di pertinenza dell'azienda nelle apposite aree disco comuni appositamente predisposte dall'IT.

8.2. Violazione dei dati (c.d. data breach)

Con la nozione di violazione dei dati personali (c.d. "*personal data breach*"), si intende: **la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso, in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati**.

I Titolari del trattamento, in caso di una violazione come sopra descritta, dovranno mettere in atto due differenti azioni:

1) la notificazione della violazione **all'Autorità di controllo** entro 72 ore dal fatto (art. 33 GDPR che prevede

che il titolare del trattamento, ai sensi dell'art. 33 GDPR deve notificare la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo).

2) la segnalazione **al diretto interessato** (senza ritardo ingiustificato – art. 34 GDPR).

Le violazioni dei dati personali possono essere costituite esemplificativamente da:

- accesso abusivo ai dati;
- copiatura dei dati;
- sottrazione dei dati;
- distruzione o modifica dei dati.

Per tali motivi, chiunque, nell'ambito della propria attività aziendale venga a conoscenza di una violazione dei dati personali deve darne comunicazione con immediatezza - e comunque entro 72 ore dalla conoscenza del fatto - al proprio responsabile o direttamente al DPO-RPD (Responsabile della Protezione dei Dati) per la gestione del *data breach* secondo la apposita procedura aziendale.

8.3. Furto o smarrimento di dispositivi informatici

In caso di furto o smarrimento dei dispositivi informatici forniti dall'azienda l'incaricato dovrà, nel più breve tempo possibile e comunque entro 72 ore dalla conoscenza del fatto:

- Seguire quanto previsto al punto 8.2 che precede per il caso di *data breach*;
- Presentare idonea denuncia di furto/smarrimento avanti alle Autorità competenti secondo le istruzioni fornite dal titolare, eventualmente per il tramite del DPO o del gestore IT dell'azienda;
- Approntare le misure di sicurezza informatiche (ad es. blocco degli account, sostituzione delle password degli account, misure di *disaster recovery,* secondo le istruzioni fornite dal titolare, eventualmente per il tramite del DPO o del gestore IT dell'azienda.

8.4. Procedura di *disaster recovery*

In caso di furto, danneggiamento o smarrimento di dati e/o di dispositivi informatici il gestore IT dovrà avviare le procedure di *disaster recovery* delineate nell'apposita procedura interna.

9. REGOLE SPECIFICHE PER LO SMART WORKING

Lo smart working (o "lavoro agile") consiste in una prestazione di lavoro subordinato caratterizzata dall'assenza di una postazione fissa durante i periodi di lavoro svolti anche al di fuori dei locali aziendali, circostanza che diversifica lo smart working dal telelavoro.
Lo smart working si svolge con le seguenti modalità:

a) prestazione lavorativa al di fuori della propria postazione abituale;
b) utilizzo di strumenti informatici e/o telematici per lo svolgimento dell'attività lavorativa;
c) senza l'obbligo di una postazione fissa o di un luogo predeterminato durante i periodi di lavoro che vengono svolti al di fuori dei locali aziendali.

Lo smart working è una modalità di lavoro innovativa, basata su un forte elemento di flessibilità, in modo particolare di orari e di sede; al lavoratore viene lasciata ampia libertà di auto-organizzarsi a patto che porti a termine gli obiettivi/progetti concordati/stabiliti nelle scadenze previste.
Le regole di comportamento previste al presente paragrafo integrano e non sostituiscono le vigenti pattuizioni collettive o individuali stipulate con i dipendenti di ASTEM S.p.A.
In particolare, risulta integralmente richiamato quanto previsto negli accordi individuali di lavoro agile stipulati ai sensi degli artt. 18 e ss. L. 81/2017 con i dipendenti.
In caso di esecuzione delle prestazioni lavorative in smart working restano inoltre ferme, ove applicabili, tutte le regole stabilite ai paragrafi precedenti.
In aggiunta varranno le seguenti regole integrative.

9.1. Efficienza ed integrità di strumenti/dispositivi e attrezzature/apparecchiature prima dell'uso.

Prima di iniziare le attività, l'utente deve verificare che:

- i cavi di alimentazione delle attrezzature elettriche siano adeguatamente protetti contro le azioni meccaniche (oggetti taglienti, ecc.) e termiche (caloriferi, ecc.);
- l'attrezzatura di lavoro non presenti eventuali cavi danneggiati e con parti conduttrici a vista.

9.2. Utilizzo delle attrezzature di lavoro/apparecchiature (istruzioni d'uso).

Prima di iniziare le attività con PC, notebook o tablet, l'utente dovrà leggere il manuale di istruzioni, attenersi scrupolosamente alle istruzioni d'uso e manutenzione per la parte in materia di salute e sicurezza del manuale.
In caso di funzionamento anomalo e/o guasto delle attrezzature/apparecchiature utilizzate proprie e/o ricevute, l'incaricato dovrà:

- mettere in sicurezza l'apparecchiatura;
- avvisare il proprio responsabile.

Il lavoratore assume espressamente l'impegno ad utilizzare gli strumenti aziendali ed i programmi informatici messi a sua disposizione esclusivamente nell'interesse del datore di lavoro, a rispettare le relative norme di sicurezza, a non manometterli e a non consentire ad altri l'utilizzo degli stessi.
Al fine di garantire la salute e la sicurezza, il datore di lavoro informa il lavoratore sui rischi generali e specifici connessi alla particolare modalità di esecuzione del rapporto di lavoro. Il lavoratore si atterrà alle indicazioni e coopererà secondo tutte le sue possibilità per fronteggiare i rischi connessi all'esecuzione della propria prestazione all'esterno dei locali aziendali.

9.3. Requisiti minimi su impianti di alimentazione elettrica - indicazioni sul corretto utilizzo dell'impianto elettrico (buono stato dei cavi elettrici di collegamento e loro posizionamento, utilizzo prese, sovraccarico, prevenzione incendi, ecc.)

Per un uso in sicurezza delle prese, è importante seguire le seguenti fondamentali regole:

- nelle operazioni di inserimento e disinserimento delle spine nelle prese, non toccare mai la spina con le mani bagnate e non si deve distaccarla tirandone il cavo elettrico;
- verificare che i fori delle prese presentino gli schermi di protezione;
- verificare l'integrità di prese e di interruttori;
- verificare che le prese di corrente e gli interruttori siano ben fissati ai loro supporti;
- non usare adattatori con spinotti piccoli da 10 A e fori grandi da 16 A;
- le spine di tipo Schuko possono essere inserite in prese di tipo italiano solo tramite un adattatore che trasferisce il collegamento di terra effettuato mediante le lamine laterali ad uno spinotto centrale: è assolutamente vietato l'inserimento a forza delle spine Schuko nelle prese di tipo italiano. In tal caso dal collegamento viene esclusa la messa a terra;
- in caso di utilizzo di prese multiple o "ciabatte", verificare che la potenza complessiva degli apparecchi collegati sia inferiore a quella indicata dalla presa multipla;
- non posizionare le prese multiple in luoghi dove possano essere danneggiate;
- verificare che le prese multiple utilizzate siano conformi alle norme CEI (ad esempio quelle dotate di marchio IMQ);
- non manomettere o modificare le prese multiple;
- nel caso risulti necessario l'utilizzo di un adattatore multiplo, accertarsi che venga utilizzata la versione consentita dalla normativa con due sole prese laterali;
- assicurarsi che i cavi di eventuali prolunghe in utilizzo risultino integri;
- non appoggiare mai mobili su un cavo elettrico e non far passare mai un cavo sotto tappeti o tappezzerie;
- le prolunghe dovrebbero essere usate solamente come una misura provvisoria, non come collegamento permanente e solo per alimentare apparecchi a limitato assorbimento;
- posizionare le prolunghe sul pavimento facendo correre il cavo lungo il muro in modo che non comportino pericolo d'inciampo per le persone;
- prima di procedere alla pulizia o al lavaggio di tutte le apparecchiature alimentate elettricamente, staccare sempre le spine isolando l'apparecchio dalla rete elettrica;
- dopo aver utilizzato un apparecchio è sempre opportuno staccare la spina che lo alimenta, evitando strappi violenti ed avendo cura di spegnere preventivamente l'apparecchio;
- se ci si assenta per lunghi periodi, staccare sempre le spine degli apparecchi elettrici dalle prese;
- verificare che sia disponibile una dichiarazione di conformità o autocertificazione dell'impianto elettrico.

Le sovrastanti regole oltre ad avere finalità di sicurezza della persona hanno anche la finalità di preservare lo strumento in dotazione i dati in esso contenuti.

9.4. Decalogo dello smart working

Lo smart working o "lavoro agile" impone la massima attenzione sui temi della riservatezza e presuppone che il/la dipendente rimanga sempre concentrato sulle modalità di lavoro, al fine di svolgere la propria attività (in parte all'interno dei locali aziendali e in parte all'esterno senza una postazione fissa) in modo corretto e idoneo per proteggere l'operatività e la reputazione dell'Ente. In particolare, il "Lavoro Agile" non dovrà essere effettuato, a

tal fine, al di fuori di ambienti protetti che garantiscano la necessaria riservatezza della prestazione e/o attraverso connessioni con collegamenti WIFI a reti aperte.

1) Le conversazioni tra il/la dipendente e gli altri interessati non devono essere oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità; pertanto, è obbligo del/della dipendente:

- Evitare di effettuare colloqui ad alta voce, di persona o per telefono, in presenza di soggetti non autorizzati a conoscere il contenuto della conversazione;
- Accertarsi che il coniuge o eventuali parenti e conoscenti non siano portati, anche involontariamente, a conoscenza di informazioni e processi attinenti l'attività lavorativa;
- Non utilizzare familiari o terzi per veicolare informazioni, anche se ritenute "banali", afferenti l'attività lavorativa;
- Nel caso di conversazioni telefoniche instaurate in seguito di chiamate inoltrate o ricevute, accertare, con cura, che l'interlocutore sia effettivamente un collega/cliente/fornitore legittimato e autorizzato a conoscere le informazioni oggetto della comunicazione;

2) ASTEM S.p.A., quale Titolare, stabilisce che, ai sensi dell'art. 24 comma 1 del Regolamento U.E. 2016/679, la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al Regolamento.

3) Il/La dipendente deve prestare particolare attenzione quando si trasportano da un locale all'altro, da uno stabile all'altro, da un luogo ad un altro (mediante mezzi pubblici o privati o anche a piedi) documenti contenenti dati personali.

4) Per quanto riguarda la generica conservazione dei dati personali utilizzati dal/dalla dipendente in "Lavoro Agile" il Responsabile dell'unità organizzativa deve adottare soluzioni organizzative idonee a ridurre il più possibile i rischi di distruzione, perdita e accessi non consentiti ai dati anche in ambiente privato eletto dal/dalla dipendente. Il "Lavoro Agile" non dovrà essere effettuato, a tal fine al di fuori di ambienti privati protetti, che garantiscano la necessaria riservatezza della prestazione.

5) Più in dettaglio per quanto concerne l'utilizzo di documenti cartacei contenti dati personali e prelevati dagli archivi di ASTEM S.p.A., si sottolinea che il trasferimento di dati personali all'esterno della società deve essere giustificato da necessità strettamente correlate all'esercizio dell'attività lavorativa, agli obblighi di legge o alla difesa degli interessi della società. La circolazione dei dati personali cartacei, in situazione di mobilità deve essere ridotta al minimo indispensabile; i dati devono essere raccolti in porta documenti riportanti l'identificazione del/della dipendente utilizzatore e il suo recapito telefonico.
In particolare, i documenti cartacei:

- devono essere utilizzati solo per il tempo necessari allo svolgimento dei compiti assegnati e poi ripartiti negli archivi aziendali dedicati alla loro conservazione;
- non devono essere lasciati incustoditi; pertanto, nel caso di assenza, anche momentanea, dal luogo in cui si svolge "Lavoro Agile" è necessario chiudere a chiave i locali che ospitano i dati ovvero riporli dentro un

armadio/cassetto chiuso a chiave; non devono restare, senza ragione, applicati su supporti (lavagne o simili) che possono essere visionati da persone non autorizzate;

- devono essere resi illeggibili prima di essere cestinati, qualora siano destinati a divenire rifiuti (ad es. strappando più volte la carta in modo che i contenuti diventino non decifrabili/non ricostruibili);

6) Per quanto riguarda il trattamento di dati personali mediante l'ausilio di strumenti elettronici, si richiamano le indicazioni fornite in punto all'atto dell'autorizzazione al trattamento dati e in particolare:

- La password di accesso deve essere conservata con diligenza in modo che resti riservata, evitando sotto la responsabilità del/della dipendente, che altri ne vengano a conoscenza;
- Il computer ed altri eventuali strumenti in dotazione e/o utilizzati per l'espletamento delle prestazioni di "Lavoro Agile" (P.C., smartphone, ecc.), non devono essere lasciati incustoditi ed accessibili a persone non autorizzate. In caso di allontanamento anche temporaneo dalla postazione di lavoro il/la dipendente è tenuto a disconnettere la sessione di lavoro bloccando l'operatività del computer ("ctrl-alt-canc") e/o l'accesso allo smartphone (password di blocco schermo);
- Non devono essere utilizzati dispositivi di memorizzazione esterna: come sopra riportato la documentazione inerente all'attività lavorativa dovrà risiedere esclusivamente sulle cartelle di rete, poiché tale modalità operativa è ritenuta adeguata a garantire che il trattamento è effettuato conformemente al regolamento.

7) I trattamenti effettuati dal/dalla dipendente devono rispettare il principio di necessità, pertinenza e non eccedenza rispetto alle finalità degli stessi, avere scopi espliciti, determinati e leciti, come da istruzioni fornite in punto all'atto dell'autorizzazione al trattamento dati di ASTEM S.p.A..

8) Nell'ambito delle proprie attività e in osservanza alle misure derivanti dal sistema procedurale, gestionale e tecnico instaurato da ASTEM S.p.A. per garantire la sicurezza dei dati personali, il dipendente tratta dati:

- esatti e, se necessario, aggiornati;
- archiviati in una forma che consenta l'esercizio dei diritti da parte dell'interessato di cui al Capo III del Regolamento Europeo;
- conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- ove necessario e compatibile, anonimizzati, pseudonimizzati o cifrati.

Il dipendente dovrà, altresì, adottare le cautele previste per legge (diritto all'oscuramento e anonimato) nell'eventuale trattamento dei dati soggetti a maggior tutela ovvero dati particolarmente sensibili per i diritti e le libertà degli interessati.

9) È fondamentale sottolineare che è severamente sanzionata dal Regolamento (UE) 2016/679 la violazione dei dati personali, cioè 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. Tale violazione può afferire a una "violazione della riservatezza", in caso di divulgazione o accesso accidentale ai dati personali, alla "perdita della disponibilità" (comprese le ipotesi di sottrazione e/o furto), in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata) e alla "violazione dell'integrità", in caso di alterazione non autorizzata o accidentale dei dati personali.

La violazione, in rapporto alla sua gravità, può comportare per l'Ente la Notifica del Data Breach, cioè la comunicazione della violazione dei dati personali all'Autorità di Controllo (Garante per la protezione dei dati personali), nonché, qualora ne abbiano un danno, ai soggetti i cui dati sono stati violati. A tal fine si ribadisce l'obbligo del/della dipendente di segnalare qualunque ipotesi di violazione dei dati personali al responsabile della struttura preposto e al Responsabile della Protezione dei Dati, tempestivamente e, comunque, nei termini previsti dalla normativa interna aziendale in materia, anche al fine di consentire il rispetto dei ristretti termini di notifica all'Autorità di Controllo previsti dal Regolamento (UE) 2016/679, ove atto dovuto.

10) Il/La dipendente è specificatamente autorizzato al trattamento, informato/a e formato/a dal Datore di Lavoro (Titolare) in merito alle peculiarità del trattamento dei dati personali conseguenti alla modalità "Lavoro agile" della Sua prestazione lavorativa ed ai conseguenti rischi e misure di sicurezza adottate e da adottarsi, che integrano quelle fornite all'atto dell'autorizzazione ai trattamenti di competenza, in relazione al ruolo ricoperto in ASTEM S.p.A.. È obbligazione contrattuale del/della dipendente rispettare dette istruzioni e partecipare alle attività formative previste di ASTEM S.p.A. in punto.

11) Il/La dipendente è consapevole ed accetta che ASTEM S.p.A. verifichi il rispetto delle misure di sicurezza informatiche ed operative che Gli/Le sono state indicate all'atto dell'autorizzazione alla modalità operativa del "Lavoro Agile", nel rispetto delle previsioni della normativa vigente in materia e dell'art.4 della L.300/70 e s.m.i..