REGOLAMENTO CONFEDERALE
SUL TRATTAMENTO DEI DATI PERSONALI

Sommario

Art. 1. Principi generali e ambito di applicazione.

1. La CGIL, in attuazione dell'articolo 16 dello Statuto, in qualità di titolare del trattamento, è il soggetto che garantisce che i trattamenti di dati personali svolti nell'intera Confederazione si svolgano nel rispetto dei diritti e delle libertà fondamentali della persona nonché della lavoratrice e del lavoratore, nonché della loro dignità, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il presente Regolamento, previsto dall'articolo 16 dello Statuto, è finalizzato a disciplinare in via generale il trattamento dei dati personali nell'intera Confederazione e delinea i principi fondamentali ai quali devono attenersi le singole strutture della Confederazione nel trattamento dei dati e i Centri Regolatori nell'adozione delle Linee Guida per il trattamento dei dati personali.

3. La CGIL, con deliberazione della Segreteria del Centro Confederale, anche su proposta del Responsabile della Protezione dei Dati, può adottare specifiche Linee Guida su singoli istituti disciplinati dalla normativa in materia di protezione dei dati, nonché Disciplinari e/o Regolamento attuativi, che dovranno essere inserite nella Sezione Privacy della Intranet CGIL e che le strutture, i soggetti autorizzati al trattamento, così come i singoli iscritti, sono tenuti a rispettare.

4. Restano ferme le attribuzioni delle rispettive responsabilità così come disciplinate nell'Accordo di Contitolarità.

Art. 2. Definizioni e principi generali del trattamento dei dati.

1. Ai fini del presente Regolamento si applicano le definizioni di cui all'articolo 4 del Regolamento UE, di cui all'art. 2-*bis* e 2-*ter*, comma 4, del Codice e, comunque, si intende per:

- **a)** **RGPD**: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati);
- **b)** **Codice**: il decreto legislativo 30 giugno 2003 n. 196 rubricato "*Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*";
- **c)** **Accordo di contitolarità**: l'accordo stipulato tra i contitolari del trattamento il 30/06/2019 e/o sue eventuali modifiche e/o nuove versioni;
- **d)** **DPO**: il Responsabile della Protezione dei Dati designato dalla CGIL ai sensi degli articoli 37, 38 e 39 del Regolamento UE, contattabile all'indirizzo PEO privacy@cgil.it;
- **e)** **Segretario Organizzativo Delegato**: il componente della Segreteria delegato ai sensi dell'art. 3, comma 2;
- **f)** **Referente Privacy**: il soggetto indicato nell'articolo 4, comma 1, del presente Regolamento;
- **g)** **Amministratore di Sistema**, anche denominato **ADS**: il soggetto individuato ai sensi dell'art. 5 del presente Regolamento;

h) **Soggetti Autorizzati**: i dipendenti, i collaboratori a qualsiasi titoli, e qualsiasi soggetto di cui all'art. 2-*quaterdecies* del Codice autorizzato al trattamento dei dati ai sensi dell'art. 7 del presente regolamento;
i) **Garante**: il Garante per la protezione dei dati personali di cui all'art. 2-*bis* del Codice.

2. Le singole strutture della Confederazione provvedono al trattamento dei dati personali nel rispetto delle disposizioni previste dall'articolo 5 del RGPD, delle eventuali Linee Guida approvate dal Centro Confederale, e comunque anche tramite la formazione dei soggetti autorizzati al trattamento.

3. I sistemi informativi e i programmi per elaboratore sono configurati riducendo al minimo l'utilizzo di dati personali e, in ogni caso, dei dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi, dati pseudoanonimizzati o dati non aventi natura particolare od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 3. Titolare e responsabili del trattamento.

1. Nell'ambito della Confederazione sono titolari del trattamento le singole strutture sindacali, individuabili nelle seguenti:

a. il Centro Confederale;
b. le singole Federazioni e i singoli Sindacati Nazionali di Categoria;
c. le singole CGIL Regionali;
d. le singole Camere del Lavoro Territoriali e/o Metropolitane;
e. le singole Federazioni o Sindacali regionali di categoria
f. le singole Categorie territoriali;
g. lo SPI Nazionale;
h. ciascuno SPI Regionale
i. ciascuno SPI territoriale

2. La funzione di rappresentanza di ciascun titolare del trattamento è svolta dal Segretario Generale della singola struttura. Il Segretario Generale può conferire delega ad un componente della Segreteria, conferendogli specifico potere di rappresentanza per la conclusione di contratti e, in genere, atti giuridici in materia di protezione dei dati e, comunque, per porre in essere atti e negozi giuridici in materia di protezione dei dati personali.

3. La singola struttura competente alla designazione del Responsabile del Trattamento ai sensi dell'Accordo di contitolarità vi provvede per il tramite del

Segretario Generale, del Segretario Organizzativo Delegato o, in alternativa, del soggetto al quale è stata attribuita la delega alla sottoscrizione del contratto o, comunque, dell'atto a fronte del quale sorge la necessità di procedere alla designazione.

Art. 4. Referenti Privacy dei Centri Regolatori.

1. Fermo restando la delega di cui al precedente articolo 3, comma 2, ciascun Centro Regolatore, con decisione della Segreteria, è tenuto ad individuare e nominare un soggetto dipendente o, comunque, legato da rapporto di collaborazione al Centro stesso che non abbia durata predeterminata nel tempo, al quale attribuire compiti di natura non politica e privi di rappresentanza allo scopo di procedere agli adempimenti in materia di protezione dei dati per il Centro Regolatore stesso e, laddove si tratti di un Centro Regolatore Regionale, delle singole strutture regionali e territoriali di competenza.

2. È facoltà del singolo Centro Regolatore nominare ulteriori Referenti, anche distinti per territorio o per compiti, qualora lo richiedessero particolari esigenze organizzative territoriali o strutturali, o particolari caratteristiche di specifiche attività di trattamento.

3. Il Referente Privacy, attenendosi alle istruzioni del Titolare e/o del DPO, nei limiti degli atti per i quali non sia necessario l'esercizio del potere di rappresentanza o di spesa, deve:

- **a)** porre in essere ogni atto necessario per osservare e fare osservare (a) la normativa in materia di protezione dei dati eurounitaria, nazionale e, se necessario, degli altri Paesi UE; (b) la normativa interna, comunque denominata (Regolamento Confederale sul Trattamento dei Dati, Disciplinare, Linee Guida, Istruzioni, note, circolari, ecc.) in materia di protezione, di finalità, di modalità di trattamento dei dati; (c) le istruzioni di carattere generale impartite dalla CGIL e/o da ciascuna delle sue strutture a tutti i soggetti autorizzati al trattamento dei dati personali; (d) eventuali ulteriori specifiche istruzioni in relazione a specifici ambiti di competenza.
- **b)** porre in essere ogni atto e comportamento necessario per garantire che i soggetti autorizzati presso la struttura rispettino le vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure interne, segnalando al DPO nonché al

Segretario Generale del Centro Regolatore, o al suo Segretario Organizzativo Delegato, ogni eventuale inosservanza;

c) fornire indicazioni e sorvegliare affinché nella struttura di competenza non vengano svolti trattamenti autonomi di dati e affinché non vengano trattati dati personali per finalità diverse da quelle per le quali sono stati raccolti e successivamente trattati, segnalando al DPO nonché al Segretario Generale del Centro Regolatore, o al suo Segretario Organizzativo Delegato, ogni eventuale inosservanza.

d) verificare la liceità e la correttezza dei trattamenti effettuati, anche attraverso controlli periodici, e verificare la qualità e la quantità dei dati oggetto dei trattamenti di competenza con specifico riferimento ai requisiti di esattezza, aggiornamento, pertinenza, non eccedenza rispetto alle finalità del trattamento, segnalando al DPO nonché al Segretario Generale del Centro Regolatore, o al suo Segretario Organizzativo Delegato, ogni eventuale inosservanza;

e) verificare che la struttura abbia designato i responsabili del trattamento di cui all'art. 28 del RGPD, stipulando il contratto o l'atto giuridico di cui al medesimo art. 28, par. 3 e 4, eventualmente segnalando tale necessità e acquisendo il parere del DPO ai fini della necessità di procedere alla designazione e sulla conformità alla normativa, alla prassi, e alle necessità del caso concreto, dell'atto di designazione;

f) fornire indicazioni e dare disposizioni, anche in accordo o su richiesta o previo parere del DPO, per l'adeguamento alle misure di sicurezza organizzative di cui all'art. 32 del RGPD, anche indicando al Segretario Generale o al Segretario Organizzativo Delegato la necessità di procedere all'acquisto delle strumentazioni ritenute necessarie dall'ADS o dal medesimo DPO;

g) provvedere all'attuazione, nell'ambito del Centro Regolatore o delle strutture orizzontali o verticali di competenza, delle procedure e delle Linee Guida per la corretta gestione dei dati assicurando che i soggetti interessati (es. iscritti, dipendenti, fornitori, ecc.) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del RGPD;

h) porre in essere gli atti necessari per autorizzare al trattamento dei dati personali i singoli soggetti che devono procedere al trattamento;

i) vigilare sulla conformità dell'operato dei soggetti autorizzati alle istruzioni, alle indicazioni, all'autorizzazioni, alle Linee Guida e, in genere, alla normativa sindacale, nazionale ed eurounitaria in materia di

trattamento dei dati personali segnalando alla Commissione di Garanzia i soggetti autorizzati che, nel trattamento dei dati, violano la predetta normativa;

j) qualora tra le attività della Struttura vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, provvedere a porre in essere gli atti necessari affinché detti soggetti vengano ritualmente designati quali Responsabili del trattamento ai sensi dell'art.28 del RGPD;

k) laddove siano di competenza, in relazione alle norme dell'Accordo di contitolarità, della singola struttura confederale, procedere a porre in essere ogni atto necessario affinché, laddove necessaria, venga effettuata la valutazione di impatto di cui all'articolo 35 del RGPD, affinché la stessa venga sottoposta al parere del DPO e, laddove da quest'ultimo ritenuta necessaria, affinché si proceda alla consultazione preventiva di cui all'articolo 36 del RGPD;

l) informare il soggetto competente alla predisposizione dei relativi atti, secondo le modalità previste dalla Linee Guida in materia, dell'avvenuta violazione dei dati personali di cui all'articolo 33 del RGPD, collaborando alla predisposizione della notifica al Garante, alla comunicazione agli interessati, e alla corretta compilazione del Registro delle Violazioni, nonché porre in essere ogni atto necessario, laddove necessaria, per la comunicazione agli interessati di cui all'art. 34 del RGPD;

m) provvedere affinché vengano annotate, nel Registro delle Attività di trattamento, le attività di trattamento in essere, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelle esistenti;

n) provvedere a determinare le modalità per procedere alla formazione dei soggetti autorizzati in materia di trattamento dei dati personali, anche coordinandosi con il DPO, e organizzare la stessa nell'ambito del Centro Regolatore e delle sue strutture orizzontali e verticali;

o) provvedere ad ogni altro atto o adempimento necessario per l'applicazione ai trattamenti di dati del RGPD, del Codice, e/o di ogni altra norma in materia, eurounitaria e nazionale, anche in relazione alle indicazioni del Titolare o del DPO, collaborando a tal fine con quest'ultimo e, ai sensi dell'art. 31 del RGPD, con il Garante per la protezione dei dati;

p) provvedere ad ogni adempimento gli sia indicato dal DPO, fermo restando la possibilità di rivolgersi al Titolare, nel rispetto di quanto

previsto dall'Accordo di contitolarità, laddove non condivida o non ritenga di adempiere alle indicazioni del DPO medesimo;

q) segnalare con tempestività al Titolare e/o al DPO eventuali problemi relativi all'applicazione della disciplina di cui al RGPD, al Codice e alla normativa confederale in materia di protezione dei dati riscontrati nell'esercizio delle attività di competenza.

4. La nomina del Referente Privacy deve essere comunicata dal Centro Regolatore al Centro Confederale e al DPO (privacy@cgil.it).

Art. 5. Amministratore di Sistema.

1. Ciascun Centro Regolatore procede alla nomina di uno o più Amministratori di Sistema, a mezzo atto scritto che contenga le specifiche funzioni attribuitegli, nel rispetto della normativa nazionale in materia e delle indicazioni del DPO. I Centri Regolatori Regionali possono attribuire ad uno o più ADS competenze sui sistemi informatici e informativi delle altre strutture orizzontali e verticali della CGIL Regionale, o alcune di esse.
2. La Categorie o Federazioni o SPI regionali i cui sistemi informatici e informatici siano autonomi rispetto a quelli della CGIL Regionale possono designare un proprio ADS.
3. Laddove il Centro Regolatore Regionale non abbia provveduto ai sensi del comma 1, secondo periodo, l'ADS deve essere designato dalla singola Camera del Lavoro, con competenza anche per i sistemi informatici e informativi delle strutture verticali e orizzontali territoriali, o per alcune di esse.
4. Le Categorie o Federazioni o SPI territoriali i cui sistemi informatici e informatici siano autonomi rispetto a quelli della Camera del Lavoro possono designare un proprio ADS.
5. L'Amministratore di Sistema:
   a) sovrintende le risorse del sistema informatico centralizzato (hardware e software) e ne consente l'utilizzo a tutti i responsabili e i soggetti autorizzati che ne abbiano titolo, mediante l'adozione delle misure di sicurezza tecniche di cui all'art. 32 del RGPD;
   b) garantisce la gestione e manutenzione degli strumenti elettronici di competenza della struttura che lo ha designato o per le quali lo ha designato;
   c) garantisce la protezione dei dispositivi e dei programmi contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del

codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare secondo la cadenza ritenuta necessaria in conformità all'art. 32 del RGPD;

d) garantisce gli aggiornamenti periodici, con la cadenza ritenuta più sicura, dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti;
e) garantisce il salvataggio dei dati con frequenza almeno quotidiana e, comunque, in modo tale da garantire tempestivamente il ripristino, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
f) adotta idonee misure che assicurino l'integrità e la disponibilità dei dati;
g) adotta idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a quattro giorni;
h) in caso di trattamento di categorie particolari di dati, predispone, se necessario, misure di pseudonimizzazione e/o cifratura dei dati personali, anche garantendo il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati;
i) predispone misure di sicurezza finalizzate a garantire che la dismissione e la distruzione dei supporti che contengono dati personali avvenga nel rispetto del provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, pubblicato in G.U. n. 287 del 9 dicembre 2008 e successive eventuali modifiche e/o integrazioni e/o nuove versioni;
j) collabora con il Referente privacy per la redazione, la conservazione e l'aggiornamento del Registro delle attività del trattamento;
k) collabora con il soggetto all'uopo delegato, relativamente alle attività di trattamento automatizzate, alla predisposizione della valutazione di impatto di cui all'articolo 35 del RGPD;
l) implementa ogni misura finalizzata al rispetto del Disciplinare sull'uso dei Servizi Informatici;
m) collabora ai fini dell'istruttoria necessaria alla notifica al Garante prevista dall'art. 33 del RGPD, alla comunicazione agli interessati e per provvedere all'adozione delle misure tecniche necessarie per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati e per prevenire analoghe violazioni future o, comunque, per provvedere agli adempimenti eventualmente suggeriti dal DPO e/o dal Referente Privacy.

Art. 6. Autorizzazione al trattamento.

1. I dipendenti, i collaboratori, i consulenti e chiunque, a qualsiasi titolo, procede al trattamento dei dati di titolarità della Confederazione, o delle singole Strutture di essa, tenuti al rispetto del presente Regolamento, sono autorizzati al trattamento dei dati personali degli iscritti, dei fornitori, dei dipendenti e di tutti coloro i cui dati personali sono oggetto di trattamento dalla Confederazione, nei limiti delle sole finalità, per lo svolgimento delle sole operazioni e per il trattamento dei soli dati necessarie e necessari per lo svolgimento delle loro attività.

2. Fermo restando quanto previsto al comma 8, le Strutture di cui al comma 1 sono tenute ad informare i singoli Soggetti autorizzati del contenuto del presente articolo, dell'ambito del trattamento consentito e delle istruzioni per procedere al trattamento.

3. Le informazioni, le comunicazioni e le istruzioni di cui al comma 2 possono essere date ai soggetti autorizzati che svolgono attività di trattamento presso le Camere del Lavoro e/o presso le Categorie, le Federazioni e gli SPI regionali e territoriali, oltre che dai soggetti indicati nell'Accordo di contitolarità, anche dalla CGIL Regionale di riferimento, previa delibera assunta dalla Segreteria di quest'ultima struttura.

4. Le informazioni, le comunicazioni e le istruzioni di cui al comma 2 possono essere comunicate mediante inserimento o allegazione al contratto, convenzione, atto unilaterale, o altro atto giuridico che regola il rapporto tra la struttura e il soggetto autorizzato o, comunque, possono essere comunicate, aggiornate o integrate mediante atto scritto consegnato a ciascun soggetto autorizzato in cartaceo, con sottoscrizione di copia per ricevuta.

5. La singola Struttura può inoltre informare, comunicare e istruire ai sensi del comma 2 in forma automatizzata, in particolare, alternativamente:

- **a)** con inviato a mezzo posta elettronica all'indirizzo email istituzionale;
- **b)** mediante visualizzazione dell'atto al primo accesso utile al sistema informatico e/o informativo della singola struttura o della Confederazione che richieda la certificazione dell'avvenuta lettura da parte del soggetto autorizzato stesso.

6. L'autorizzazione al trattamento ai Soggetti autorizzati che non siano tenuti al rispetto del presente Regolamento, e le conseguenti istruzioni, può avvenire mediante atto contenuto o allegato al contratto, convenzione, atto unilaterale, o altro atto giuridico che regola il rapporto tra la struttura e il soggetto autorizzato che preveda l'obbligo per il medesimo Soggetto

autorizzato di leggere e rispettare il presente Regolamento e, comunque, la normativa e la prassi del sindacato in materia sindacale e di protezione dei dati.

7. Le istruzioni per il trattamento dei dati devono essere collocate in luogo facilmente e permanentemente accessibile da parte di ciascun Soggetto Autorizzato, anche per le finalità di cui all'art. 7 della legge 300/1970.

8. In ogni caso l'atto di autorizzazione contiene l'avvertimento al Soggetto Autorizzato della necessità di:

- **a)** garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza;
- **b)** attenersi alle istruzioni impartite dal Titolare, dal DPO e dal Referente Privacy;
- **c)** effettuare il trattamento in ottemperanza ai principi di liceità, correttezza, pertinenza e non eccedenza dei trattamenti effettuati, con specificazione sintetica del significato di ciascun singolo principio;
- **d)** trattare i dati per le sole finalità strettamente inerenti all'oggetto dell'incarico;
- **e)** evitare di comunicare i dati trattati a soggetti ai quali la comunicazione non è consentita;
- **f)** prendere visione e rispettare le istruzioni, i Regolamenti, i Disciplinari, le Linee Guida e, in genere, le istruzioni e le circolari in materia di trattamento dei dati personali resigli noti e/o pubblicati nella Sezione Privacy del sito Intranet della CGIL;
- **g)** partecipare agli incontri e alle iniziative di formazione organizzati periodicamente dal Centro Regolatore o, comunque, dalla singola struttura sindacale.

9. I Soggetti Autorizzati sono tenuti a frequentare gli incontri formativi organizzati periodicamente dalla Confederazione ai sensi dell'articolo 18.

10. In caso di violazione del comma 9 o, comunque, in caso di mancato conseguito della certificazione di frequenza e superamento dei relativi test finali il Referente Privacy è tenuto a dare disposizioni affinché vengano venga sospesa l'autorizzazione al trattamento dei dati o, comunque, avrà cura di impedire il trattamento dei dati fino da parte dell'operatore inadempiente fino all'effettiva frequenza e all'effettivo apprendimento delle nozioni di cui ai commi precedenti.

Art. 7. Modalità di raccolta e requisiti dei dati.

1. I soggetti autorizzati al trattamento sono tenuti a trattare i dati nel rispetto delle disposizioni di cui all'articolo 5 del RGPD ("*Principi applicabili al trattamento di dati personali*").
2. I soggetti autorizzati al trattamento sono tenuti a raccogliere e registrare i dati da trattare in forma automatizzata attraverso gli strumenti elettronici messi a disposizione dalla Confederazione e/o dai Centri Regolatori.
3. Il soggetto autorizzato alla raccolta dei dati personali che avviene al momento della domanda di iscrizione alla CGIL è tenuto ad accertare l'identità del soggetto che la propone, eventualmente anche mediante richiesta di esibizione di un documento di identità, anche finalizzata alla verifica dei dati personali, ma avendo cura di non procedere alla raccolta dei dati non necessari.

Art. 8. I diritti dell'interessato.

1. L'adempimento delle richieste formulate dall'interessato ai sensi degli articoli 12 e seguenti del RGPD, e il riscontro agli interessati stessi, avviene, a cura del Referente Privacy del Centro Regolatore di competenza, nei termini e secondo le modalità determinate dalle eventuali Linee Guida adottate dalla Segreteria di ciascun Centro Regolatore ovvero, in mancanza, dalle Linee Guida adottate dalla Segreteria del Centro Confederale.
2. Il singolo Centro Regolatore, nell'ambito delle predette Linee Guida, può affidare al DPO il compito di riscontrare le richieste degli interessati, fermo restando i necessari rapporti contrattuali con il DPO medesimo.
3. In ogni caso, presso ciascun Centro Regolatore, è istituito il Registro dei Diritti dell'Interessato nel quale verranno annotate:
    a. la data di ricezione dell'istanza;
    b. il nominativo dell'interessato e dell'istante (se diverso dal primo)
    c. la descrizione della richiesta;
    d. la struttura o le strutture coinvolte e le eventuali banche dati coinvolte;
    e. l'azione intrapresa;
    f. la data del riscontro all'interessato;
    g. eventuali note o commenti, nelle quali verrà indicato l'eventuale parere del DPO.

4. Nell'ambito delle Linee Guida elaborate dal Centro Regolatore viene individuato il luogo e le modalità della conservazione delle istanze dell'interessato.
5. Il Referente Privacy competente al riscontro che abbia dubbi sulle modalità per provvedere, potrà avvalersi della consulenza del DPO.
6. L'interessato che eserciti i diritti previsti dagli articoli 12 e seguenti del RGPD dovrà essere identificato sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura o di delega sottoscritta dall'interessato nelle forme di cui all'articolo 38 del DPR 445/00.
7. L'eventuale richiesta verbale da parte dell'interessato dovrà essere annotata a cura del Referente e/o del personale autorizzato.
8. Il personale autorizzato che riceva una richiesta di cui al presente articolo è tenuto a trasmetterla con immediatezza al Referente Privacy di competenza.

Art. 10. Informazioni agli interessati.

1. I Referenti Privacy sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del RGPD nel rispetto delle indicazioni fornite dal Centro Confederale Nazionale e/o dal DPO.
2. Fermo restando quanto previsto al comma precedente, le predette informazioni sono fornite al momento della domanda di iscrizione attraverso il modello predisposto dal Centro Confederale Nazionale.
3. Nell'ambito delle attività di trattamento che comportano la raccolta dei dati per finalità per le quali non sono già state fornite in precedenza, le informazioni di cui agli articoli 13 e 14 del RGDP, le stesse devono essere fornite mediante la loro indicazione nella stessa documentazione che viene consegnata all'interessato o che l'interessato è tenuto compilare. In mancanza le predette informazioni sono fornite attraverso apposita cartellonistica collocata in modo tale che sia visibile all'interessato che fornisce i dati, anche utilizzando il sistema della c.d. "informativa a strati" e/o le icone standardizzate pubblicate nella pagina https://www.garanteprivacy.it/temi/informativechiare#2.
4. Inoltre, le predette informazioni dovranno essere rese:
   a) nell'ambito delle attività di trattamento connesse al rapporto di lavoro e/o di collaborazione e/o di volontariato, nella modulistica che viene

consegnata all'interessato all'atto della formalizzazione del rapporto di lavoro, di collaborazione o di volontariato;

b) nell'ambito delle attività di trattamento dei dati di soggetti non iscritti (es. nel contesto della raccolta dei dati dei lavoratori ai fini dell'organizzazione delle elezioni RSU), inviando una email ai lavoratori i cui dati sono stati raccolti;

c) per i trattamenti di dati svolti nel contesto dei siti internet istituzionale, mediante pubblicazione delle informazioni stesse nel sito Internet.

5. La struttura che procede ad attività di trattamento per le quali ritiene necessario prevedere specifiche modalità per fornire le informazioni di cui agli articoli 13 e 14 del RGPD, ai fini delle informazioni da rendere e/o per determinare le modalità per fornirle è tenuto ad avvalersi della consulenza del DPO.

Art. 11. Analisi dei rischi, valutazione di impatto e consultazione preventiva.

1. La struttura tenuta alla valutazione di impatto ai sensi dell'art. 7 dell'accordo di contitolarità vi procede a cura del Referente Privacy, che può incaricare l'ADS o, se ritiene, un soggetto esterno con specifiche competenze in materia.
2. All'esito della valutazione di impatto il Referente Privacy chiede il parere sulla stessa al DPO, inviandogliela al dato di contatto privacy@cgil.it.
3. Il Referente Privacy avrà cura di fornire le istruzioni necessarie per procedere alle attività di trattamento in conformità alla valutazione di impatto e al successivo parere del DPO, salvo diversa indicazione della Segreteria del Centro Regolatore di competenza.
4. Laddove il DPO ritenga necessaria la consultazione preventiva del Garante prevista dall'art. 36 del RGDP, la stessa è richiesta dal Segretario Generale o dal Segretario Organizzativo Delegato in conformità alle indicazioni del DPO, salvo diverso parere della Segreteria del Centro Regolatore di competenza.
5. Laddove non sia necessaria la valutazione di impatto, la struttura è comunque tenuta ad effettuare una valutazione dei rischi, da documentare e allegare al Registro delle Attività di Trattamento.
6. Resta fermo quanto previsto dall'art. 12 dell'accordo di contitolarità.

Art. 12. Misure di sicurezza applicabili al trattamento non automatizzato dei dati.

1. Le singole strutture e, comunque, i soggetti autorizzati al trattamento sono tenuti:

a. a trattare i soli dati essenziali per svolgere l'attività sindacale, riducendo al minimo l'utilizzo dei dati particolari e l'utilizzo dei dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati di natura non particolare, dati pseudoanonimi o dati anonimi o, comunque, dati di natura meno invasiva od opportune modalità che permettano di identificare l'interessato solo in caso di necessità;
b. introdurre e controllare i dati in modo da ridurre al minimo i rischi di distruzione e perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla qualità della raccolta, tramite l'applicazione di misure di sicurezza adottate dall'Amministratore di Sistema, anche su parere del DPO, in conformità all'articolo 32 del RGPD ed anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, secondo le indicazioni impartite dallo stesso Amministratore di Sistema.

2. I dati su supporto cartaceo devono essere conservati in luoghi o contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento. In ogni caso gli atti e i documenti devono essere conservati in archivi ad accesso selezionato e gli incaricati debbono conservarli e restituirli al termine delle operazioni effettuate.

3. Nel caso di trattamenti di dati particolari di cui agli articoli 9 (dati particolari) e 10 (dati giudiziari) del RGPD, oltre a quanto sopra previsto debbono essere osservate le seguenti modalità:

a. gli atti e documenti debbono essere conservati in locali o contenitori muniti di serratura ai quali non abbiano accesso soggetti diversi da quelli autorizzati, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti;

b. l’accesso agli archivi deve essere controllato e devono essere identificati e registrati i soggetti che vi accedono dopo l’orario di chiusura degli archivi stessi.

4. La singola struttura è tenuta ad adottare le misure di sicurezza di tipo organizzativo finalizzate a ridurre al minimo il rischio di distruzione e perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla raccolta quali, a titolo esemplificativo e non esaustivo:

a. soluzioni volte a rispettare, in relazione a prestazioni o adempimenti preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati che prescinda dalla loro individuazione nominativa (sistemi “salva coda” o che, comunque, impongano a chi è in attesa di attendere in luogo diverso da quello ove avviene il contatto tra interessato e soggetto autorizzato al trattamento);
b. l’istituzione di appropriate distanze di cortesia, tenendo conto dell’eventuale uso di apparati vocali o di barriere o, comunque, della specifica situazione logistica;
c. soluzioni che prevengano, durante colloqui, l’indebita conoscenza da parte di terzi di informazioni personali;
d. cautele volte ad evitare che la raccolta dei dati avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
e. la previsione di opportuni accorgimenti e modalità volte ad assicurare che possano essere date informazioni telefoniche;
f. previsione di sistemi di allarme e/o anticendio o, comunque, di misure che, in loro mancanza, impediscano la perdita dei dati.

5. È fatto divieto di utilizzo degli apparecchi fax. Laddove l’uso dei singoli apparecchi sia strettamente necessario, la struttura è tenuta a informare il DPO, che fornirà indicazioni per la trasmissione e la ricezione delle comunicazioni e affinché la relativa apparecchiatura sia collocata in un’area protetta e presidiata.

6. La trasmissione cartacea di documenti deve essere effettuata in busta chiusa e sigillata che riporti il nominativo del destinatario. Nella busta non potranno essere apposte indicazioni che consentono di presumere il contenuto della busta stessa; dovrò inoltre essere omessa l’indicazione nominativa del mittente e/o dello specifico ufficio da cui proviene la busta.

7. I documenti cartacei che contengano dati personali e dei quali non sia imposta la conservazione devono essere smaltiti attraverso appositi distruggi-documenti o, se non disponibili, distruggendo fisicamente il supporto cartaceo in modo che ne sia impedita la ricostruzione. La distruzione di ingenti quantità

di documenti cartacei deve essere effettuata attraverso l'incarico ad esperti del settore (es. società di smaltimento rifiuti) che dovranno essere designati alla responsabilità del trattamento ai sensi dell'art. 28 del RGPD.

Art. 13. Misure di sicurezza applicabili al trattamento automatizzato dei dati.

1. Il trattamento dei dati effettuato con strumenti elettronici è consentito solo nel rispetto delle Linee Guida di cui all'Allegato A.

2. In ogni caso l'Amministratore di Sistema avrà cura di prevedere, quantomeno, le seguenti misura di sicurezza:

a. autenticazione informatica, con le specifiche procedure di gestione delle credenziali di autenticazione, valutando la possibilità di implementare un sistema di autenticazione a doppio fattore;
b. utilizzazione di un sistema di autorizzazione;
c. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato e agli addetti alla gestione o alla manutenzione degli strumenti elettronici;
d. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti;
e. adozione di procedure per la custodia di copie di sicurezza, e per il ripristino della disponibilità dei dati e dei sistemi;
f. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati particolarmente sensibili.

3. La trasmissione elettronica dei dati di natura particolare potrà avvenire solo attraverso il servizio "cloud" della Struttura oppure, in mancanza, attraverso altri accorgimenti tecnici individuati dall'Amministratore di Sistema.

4. In ogni caso, laddove sia strettamente necessario la trasmissione di dati e documenti attraverso strumenti elettronici, è fatto divieto di indicare dati di natura particolare nel testo del messaggio e, comunque, i documenti allegati devono essere previamente criptati o, comunque, protetti da strumenti che ne impediscano l'apertura a soggetti non autorizzati.

5. Ciascun Centro Regolatore è tenuto ad adottare il Disciplinare sull'uso dei Servizi Informatici nel rispetto delle Linee Guida del Garante adottate con deliberazione n. 13 del 01/03/2007 e successive modifiche, integrazioni e/o chiarimenti.

6. Il Disciplinare adottato dai Centri Regolatori Nazionali, che dovrà essere adottato con delibera della Segreteria, sentito il DPO, ha efficacia per la sola

struttura nazionale. Il Disciplinare adottato dalle CGIL Regionali, che dovrà essere adottato con delibera del Direttivo, ha efficacia per la struttura regionale, per le Categoria e Federazioni Regionali, compreso lo SPI Regionale, per le Camere del Lavoro territoriali o metropolitane e per le Categorie, Federazioni e gli SPI territoriali.

7. Le Linee Guida di cui all'Allegato A saranno oggetto di revisione periodica, comunque mai superiore al biennio, con delibera della Segreteria del Centro Confederale Nazionale, sentito il DPO.

Art. 14. Diffusione dei dati particolari.

1. I dati di natura particolare non possono essere oggetto di diffusione.
2. È consentita la diffusione dei predetti dati nel solo caso in cui siano state resi noti dall'interessato attraverso suoi comportamenti pubblici e, comunque, per le sole finalità, nei soli casi e secondo le modalità previste dagli articoli 136 e seguenti del Codice (*Finalità giornalistiche e altre manifestazioni del pensiero*).
3. La partecipazione delle iscritte e degli iscritti ad assemblee dei lavoratori e/o, comunque, a iniziative in ambito aziendale non si considera comportamento pubblico sufficiente ai fini di quanto previsto dal comma precedente.
4. Si considerano rientranti nei dati resi noti dall'interessato attraverso suoi comportamenti pubblici la partecipazione ad iniziative collettive in luoghi pubblici o aperti al pubblico nonché l'accettazione, anche tacita, di un incarico di direzione.
5. Le registrazioni sonore e video delle riunioni degli organi statutari, e comunque delle riunioni sindacali non pubbliche e/o non aperte al pubblico, sono consentite solo su disposizione e/o autorizzazione della presidenza della riunione stesse.

Art. 15. Registro delle attività di trattamento.

1. Il Registro delle attività di trattamento previsto dall'art. 30 del RGPD, laddove possibile, deve essere redatto avvalendosi della procedura informatica elaborata dal Centro Confederale Nazionale.
2. Laddove non sia possibile avvalersi della procedura di cui al comma 1, o comunque fino all'implementazione della stessa, il Registro è conservato e aggiornato dal Referente Privacy del Centro Regolatore, il quale ne trasmette copia al DPO (al dato di contatto privacy@cgil.it) entro il 15 dicembre ogni anno.

3. Ai fini della compilazione e dell'aggiornamento del Registro, il Referente Privacy può conferire delega all'ADS e, nell'ambito del Centro Regolatore Regionale, al Segretario Organizzativo Delegato di ciascuna struttura territoriale che, a sua volta, può delegare l'ADS della struttura territoriale.
4. Le singole strutture sindacali territoriali sono tenute ad informare il Referente Privacy del Centro Regolatore Regionale di ogni nuova attività di trattamento o, comunque, della modifica delle caratteristiche delle attività di trattamento già incluse nel Registro.

Art. 16. Violazione dei dati personali.

1. I casi di violazione dei dati personali devono essere notificati al Garante, comunicati agli interessati, annotati nel Registro di cui al comma 2 e, comunque, gestiti e istruiti secondo le modalità previste dalla Linee Guida approvate dalla Segreteria del Centro Confederale Nazionale.

Art. 17. Attività di monitoraggio.

1. La CGIL svolge attività di monitoraggio e sorveglianza in ordine all'applicazione del RGPD, del Codice e delle norme confederali in materia di protezione dei dati personali, ivi comprese le relative istruzioni applicative, nei confronti di tutte le strutture confederali.
2. Il predetto monitoraggio può essere eseguito:
    a. nel corso delle ispezioni confederali, sulla base del regolamento del Collegio Ispettori;
    b. tramite la richiesta di compilazione di un questionario che può essere richiesta dal Centro Confederale Nazionale, dal Centro Regolatore di competenza, dal DPO e/o da soggetti ai quali le predette strutture abbiano conferito mandato in tal senso;
    c. direttamente, dal DPO e/o da soggetti dallo stesso incaricati;
    d. tramite accessi e ispezioni da parte dei soggetti di cui alla lett. b).
3. Le attività svolte durante il monitoraggio sono soggette a verbalizzazione riassuntiva, che deve riportare, tra l'altro, le indicazioni relative alle procedure e alle misure suggerite alla struttura per svolgere e/o proseguire le attività di trattamento.
4. Tale documentazione viene trasmessa in copia al Centro Confederale Nazionale, al Centro Regolatore di competenza e al DPO.

5. Il Referente Privacy, anche mediante controlli periodici, è tenuto a verificare costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto e alla prestazione in corso, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa.
6. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

Art. 18. Attività di formazione degli operatori.

1. Nel rispetto delle competenze e delle modalità previste dall'art. 4 dell'Accordo di contitolarità, i Centri Regolatori provvedono alla formazione periodica degli operatori, in particolare sensibilizzandoli rispetto

- al concetto e al significato di diritto alla protezione dei dati personali, fornendo indicazioni sul significato di tale diritto e sugli istituti previsti dal RGPD;
- alla possibilità e necessità di coinvolgere, in caso di dubbi, o comunque per ogni attività di trattamento, il Referente Privacy e il DPO;
- al rispetto del RGPD, della normativa nazionale e della prassi in materia, dell'Accordo di contitolarità, del presente Regolamento, del Disciplinare sull'uso dei sistemi informatici e informativi e, in generale, delle Linee Guida, delle indicazioni e della prassi della CGIL in materia di protezione dei dati;
- od ogni istituto e/o questione che sia indicata dal dal DPO o con programmazione biennale approvata dal Segretario Generale Delegato del Centro Confederale e comunicata ai singoli Centri Regolatori i quali, nel rispetto di tale programmazione, possono integrarla con istituto o questione relative alle proprie specifiche attività di trattamento o che ritengano necessari sottoporre ai propri soggetti autorizzati.

2. I Centri Regolatori provvedono altresì alla formazione specifica dei Referenti Privacy, dei Segretari Generali e Organizzativi, degli Amministratori di Sistema e loro delegati e/o, comunque, del personale amministrativo con specifiche competenze in materia di protezione dei dati, in particolare su temi e

istituti specifici relativi alla protezione dei dati, sicurezza informatica, gestione degli incidenti, tenuta del Registro delle Attività di Trattamento, Analisi dei rischi, individuazione e autorizzazione al trattamento degli operatori, gestione delle informative privacy e dei consensi al trattamento dei dati, redazione e svolgimento della valutazione di impatto, procedure e istruttoria dei casi di violazione dei dati, designazione dei responsabili del trattamento, gestione dei casi di esercizio dei diritto degli interessati e quant'altro eventualmente indicato dal DPO.

3. I Centri Regolatori potranno procedere alla somministrazione della formazione mediante personale interno e/o esterno che dia garanzia di competenza in materia di protezione dei dati. Si presumono competenti i soggetti all'uopo convenzionati con il Centro Confederale Nazionale.

4. La formazione potrà essere somministrata in presenza o a distanza. In tale ultimo caso potrà essere somministrata secondo modalità sincrona o asincrona mediante utilizzo, in entrambi i casi, di piattaforme o, comunque, modalità tecniche che certifichino la frequenza e l'effettivo apprendimento da parte dell'operatore autorizzato.

Art. 19. Consulenza del Responsabile della Protezione di Dati. Intranet sindacale.

1. Fermo restando la possibilità di rivolgersi direttamente al DPO, i soggetti autorizzati al trattamento, per qualsiasi questione, informazione, consulenza e/o dubbi in materia di trattamento dei dati personali sono tenuti a rivolgersi al Referente Privacy del Centro Regolatore di competenza.

2. Il Referente Privacy e, in ogni caso, la singola struttura confederale che abbiano necessità di consulenza in materia di protezione dei dati, sono tenuti a richiedere consulenza al DPO, scrivendo al suo dato di contatto: privacy@cgil.it.

3. Fermo restando quanto previsto dall'art. 12 dell'accordo di contitolarità, i Referenti Privacy e i soggetti autorizzati, in ogni caso, sono tenuti a conformarsi alle informative e ai pareri espressi dal DPO.

4. La normativa confederale e le indicazioni, così come la modulistica necessaria a conformarsi alle disposizioni eurounitarie, nazionali e confederali in materiali di protezione dei dati sono pubblicate nella Sezione Privacy del sito intranet del Centro Confederale Nazionale.

Art. 20. Revisione periodica del Regolamento.

1. Il presente Regolamento è soggetto a revisione periodica su indicazione del DPO o, comunque, in mancanza, con cadenza almeno quadriennale.

Allegato A
Sicurezza dell'Informazione

Requisiti di "Security Compliance"

Sommario

1. Introduzione

Questo documento definisce le linee guida e i requisiti essenziali per implementare un sistema di gestione delle informazioni, in linea con le esigenze, i livelli di sicurezza e le normative in materia di protezione dei dati, italiane ed eurounitarie.

Costituiscono essenzialmente un sottoinsieme delle indicazioni e dei controlli previsti dalla norma EN ISO/IEC 27001:2017, riguardante i Sistemi di Gestione della Sicurezza dell'Informazione (SGSI), a cui vengono aggiunti i requisiti/adempimenti specifici del RGPD.

2. Identificazione e classificazione delle informazioni (in particolare dati personali)

2.1. Censimento delle informazioni e dei supporti/archivi

Per poter avviare un processo di gestione sicura delle informazioni, è fondamentale sapere **quali informazioni si trattano** e **dove sono archiviate**.

Il censimento delle informazioni, con particolare riguardo ai dati personali, è importante soprattutto ai fini degli adempimenti previsti dal RGPD, per la creazione e aggiornamento del Registro dei Trattamenti, per la valutazione dei rischi e per l'eventuale approfondimento necessario per la Valutazione d'impatto (DPIA).

Identificare i supporti, fisici o informatici, su cui i dati risiedono è importante per **valutare le vulnerabilità e le minacce** (quindi i rischi) a cui i dati sono sottoposti.

L'analisi può essere effettuata sia partendo dal censimento delle tipologie di informazioni trattate dalle varie aree dell'Organizzazione, sulla base dei progetti, ruoli, tipologie di pratiche, ecc., sia analizzando il contenuto dei supporti, archivi fisici (armadi, faldoni, ...) o digitali (computer, server, dischi di rete, dischi rimovibili, chiavette USB, CD, spazi cloud, supporti di backup ...).

Una stessa tipologia di informazioni (es. dati personali, documenti di progetto, ecc.) può essere presente su molti supporti, in formati differenti (documento, database, email, ecc.), così come uno stesso supporto (es. un file server, un NAS, un portatile) può contenere molte tipologie di informazioni.

L'obiettivo dell'analisi è quella di avere un quadro il più possibile completo della distribuzione dei dati all'interno dell'Organizzazione, in modo da poter valutare in modo corretto i rischi e attuare le possibili azioni di protezione.

Nel caso dei dati personali, è necessario effettuare un'analisi più approfondita, in quanto le attività di trattamento svolte devono confluire nel Registro dei Trattamenti secondo le disposizioni del Regolamento.

Proprio ai fini della compilazione (o aggiornamento) del Registro dei Trattamenti, in fase di censimento dei dati vanno individuate una serie di informazioni aggiuntive, tra cui:

- Titolare/Responsabile dei dati personali individuati;
- categoria degli interessati;
- tipologia di dati oggetto dell'attività di trattamento, con specifica indicazione della categeoria di dati particolari eventualmente trattati (sindacali, politici, sanitari, sessuali, ecc…).
- destinatari dei dati;
- durata di conservazione per ciascuna finalità del trattamento;
- misure di sicurezza tecniche e organizzative adottare per la protezione dei dati;
- eventuale valutazione di rischio, sulla base delle vulnerabilità, delle minacce e della probabilità che avvenga una violazione dei dati.

Oltre agli adempimenti specifici finalizzati al rispetto del RGPD, ai fini della valutazione del rischio e per attuare in modo più efficace e mirato le misure di protezione, è utile predisporre una tabella in cui siano

censiti tutti i dispositivi e i supporti ("asset", digitali e fisici) che conservano informazioni che hanno valore per l'Organizzazione o che sono critiche, anche sulla base della valutazione fatta riguardo ai dati personali.

Dei vari supporti/archivi identificati, vanno specificati:

- identificativo del supporto (n. inventario/cespite, oppure nome dispositivo);
- tipo di supporto (es. armadio con documenti cartacei, PC utente generico, PC amministratore, NAS, ecc.);
- persona responsabile o il principale utilizzatore (dove possibile);
- tipo di informazioni contenute (dati personali/ anagrafici, dati particolari/sensibili, documenti di progetto, documenti riservati, ecc.) e formato dei dati (es. file Office, database, dati di applicazioni particolari, ecc.);
- collocazione fisica del supporto (es. locale tecnico, area accoglienza utenti, ufficio amministrazione, ecc.).

Ogni tipologia di informazione, e di conseguenza il supporto/archivio che la contiene, ha dei requisiti di sicurezza che possono essere dettagliati in base ai tre requisiti fondamentali che riguardano la sicurezza dell'informazione: **Riservatezza, Integrità e Disponibilità**.

La valutazione di questi parametri è importante per valutare l'impatto che un incidente di sicurezza può avere e per determinare le misure di protezione più idonee da adottare per la limitazione dei rischi.

2.2. Riservatezza

Indica la necessità di **non rivelare o divulgare le informazioni** ad individui, entità o processi non autorizzati.

2.2.1. Livelli di Riservatezza

Basso (R1) Informazione Pubblica	Le informazioni non presentano particolari requisiti di riservatezza. L'eventuale divulgazione o diffusione, in qualunque ambito essa avvenga, non metta a repentaglio le attività svolte dalla Società e non causa in alcun modo danni.
Medio (R2) Informazione Interna	Le informazioni devono essere accessibili solo dal personale interno alla Società, ma un'eventuale loro diffusione non ha elevati impatti sul business aziendale e non viola normative vigenti. Società esterne possono accedere a queste informazioni solo dopo aver preventivamente sottoscritto un accordo di riservatezza (Non Disclosure Agreement). Questo livello di classificazione è quello predefinito per tutte le informazioni prodotte.

Alto (R3) Informazione Riservata	Le informazioni, oltre ad essere da considerare come "interne", sono di particolare rilevanza/criticità e un'eventuale divulgazione o diffusione all'esterno non autorizzata, potrebbe avere un sensibile impatto sulle attività dell'Organizzazione, suoi sui clienti/soci, oppure causare possibili danni di immagine, azioni legali, di tipo civile o penale, danni economici. Le informazioni classificate come “Riservate” possono essere accedute, trattate e/o elaborate solo dal personale autorizzato, Rientrano in questa categoria, ad esempio, documenti tecnici che espongono dettagli che possono essere sfruttati per tentativi di violazione di sicurezza, informazioni con valore strategico per l’Organizzazione, informazioni relative a credenziali di accesso (login/password) a servizi che espongono dati critici, informazioni relative a dati personali particolari e giudiziari.

2.3. Integrità

Indica la necessità di proteggere dati e informazioni da **modifiche/cancellazioni non autorizzate o accidentali**

2.3.1. Livelli di Integrità

–Basso (I1)	Le informazioni non presentano particolari requisiti di integrità. Eventuali modifiche indesiderate o cancellazioni non comportano criticità.
–Medio (I2)	La mancanza di integrità dei dati ha un impatto limitato, cioè non comporta danni economici, violazioni di normative di legge, danni d'immagine.
–Alto (I3)	La mancanza di integrità dei dati ha elevati impatti sull'Organizzazione, in termini economici, legali (anche per violazione di norme in materia di protezione dei dati), danno d'immagine.

2.4. Disponibilità

Indica la necessità di garantire che l'informazione sia disponibile quando ne viene fatta richiesta, nelle modalità e nei tempi conformi agli obiettivi e alle policy definite dall'Organizzazione.

2.4.1. Livelli di Disponibilità

Basso (D1)	L’indisponibilità delle informazioni, anche per un tempo prolungato, non comporta danni all'Organizzazione, multe o penali.
Medio (D2)	L’indisponibilità delle informazioni oltre i tempi previsti (da contratti o processi aziendali) comporta danni economici, multe o penali, o altri danni, ma non particolarmente rilevanti.
Alto (D3)	L’indisponibilità delle informazioni oltre i tempi previsti (da contratti o processi aziendali) comporta danni rilevanti.

2.5. Analisi delle vulnerabilità e valutazione del rischio

In base all'analisi effettuata sugli archivi e sulle tipologie di dati in essi contenute, è importante valutare il livello di sicurezza, in termini di rischio a cui è sottoposto il dato di subire possibili "violazioni".

Il "rischio" in generale è valutato dal punto di vista dell'Organizzazione, ma, nel caso di dati personali, va valutato in primo luogo dal punto di vista dell'interessato (persona di cui trattiamo e tuteliamo i dati).

I fattori in gioco, che concorrono alla valutazione del rischio sono:

- **Minacce**: azioni o eventi che possono potenzialmente generare un "incidente" e compromettere i dati. Ad esempio furto, cancellazione accidentale, evento naturale, attacco informatico, malware, blackout, ecc.
- **Vulnerabilità**: debolezza o falla di sicurezza del sistema o di un processo, che potrebbe consentire ad una minaccia di essere attuata e arrecare danno. Ad esempio archivio dati lasciato incustodito, password deboli, dispositivi obsoleti, sistemi non aggiornati, mancanza di antivirus, ecc.
- **Livello di Impatto**: entità del danno che una certa minaccia potrebbe compiere su un "asset" (es. archivio di dati, dispositivo) se riuscisse ad attuarsi, sfruttando una vulnerabilità.
  Può essere espresso con una semplice scala di valori, come "basso", "medio", "alto" , a cui si può attribuire un valore numerico (I = 1, 2, 3). L'impatto dipende naturalmente anche dal "valore" che ha la tipologia di informazione che viene compromessa.
- **Probabilità**: stima la probabilità che l'incidente avvenga, cioè che una determinata minaccia possa causare un danno ad un determinato asset dell'Organizzazione. Come l'impatto, la probabilità può essere espressa con una semplice scala di valori, ad es. da 1 a 5, da "bassa" (P=1) ad "alta" (P=5).
  La probabilità va valutata principalmente in base alla possibilità che una certa minaccia sfrutti una certa vulnerabilità, ma anche considerando le misure di protezione che abbiamo adottato, la frequenza di accadimento di un evento in precedenza, l'evoluzione tecnologica, ecc.
- **Rischio**: valore che fornisce una sintetica valutazione del livello di sicurezza di un certo asset. Si ottiene dalla formula

  Rischio = Probabilità Evento x Impatto

  È legato a tutti i fattori detti sopra, che possono variare nel tempo (così come gli asset stessi su cui abbiamo fatto l'analisi): per questo la valutazione del rischio va ripetuta periodicamente.

Per un certo asset (es. un archivio cartaceo che contiene una certa tipologia di documenti), l'impatto o danno può essere valutato in maniera più precisa in base a quanto compromette ognuno dei tre requisiti fondamentali di **Riservatezza, Integrità e Disponibilità**, identificati nella fase di analisi precedente.

Di conseguenza le misure di protezione da adottare possono essere definite in modo più mirato considerando quali dei tre requisiti di sicurezza è più a rischio, in quanto più impattante. Ad esempio, per un dato sensibile all'interno di un hard disk di rete, con un impatto alto sulla riservatezza, in caso di furto o accessi non autorizzati, per abbassare il rischio si potranno adottare misure tecniche orientate a controllare meglio i permessi di accesso, a proteggere fisicamente il dispositivo, a cifrare i dati contenuti, ecc.

L'analisi dei rischi consente subito di ottenere due importanti benefici:

- individuare i **punti più deboli del sistema** (rischio più alto) e quindi poter definire un **ordine di priorità di intervento**;

- individuare le **azioni migliorative più idonee** alla riduzione del rischio, con possibilità di monitorare lo stato di avanzamento e effettuare nuovamente la stessa analisi a distanza di tempo, per **verificare l'efficacia delle azioni intraprese**.

2.6. Schema per la valutazione del rischio sulle informazioni

Si riporta a titolo di esempio, un template semplificato utilizzabile per effettuare una valutazione di rischio a partire dai supporti/archivi che conservano determinate tipologie di informazioni

Archivio/Supporto	**Incidente (Minaccia+Vulnerabilità)**	**Probabilità Incidente**	**Impatto/Danno**		**Livello di rischio**	**Azioni da pianificare per ridurre il rischio**
Archivi/supporti che conservano informazioni che hanno "valore" per l'azienda (la loro indisponibilità e/o la perdita di riservatezza o integrità possono comportare un danno). Lo stesso criterio di analisi può essere effettuato per i servizi.	Incidente (causato da minaccia e v*ulnerabilità) che potrebbe compromettere a vari livelli l'Informazione o il servizio in termini di Riservatezza, Integrità e/o Disponibilità*	*Stima della **probabilità, da 1 a 5,** che la minaccia possa attuarsi. (1=bassa; 3=media; 5=alta)*	*Liivello di "I**mpatto**" (danno), **da 1 a 5**, (1=basso; 3=medio; 5=alto), nel caso in cui la minaccia venisse attuata, in termini di **Riservatezza** (**R**), **Integrità** (**I**) e **Disponibilità** (**D**). Calcolare poi **l'Impatto Totale** come R+I+D*		Calcolare il rischio come **Probabilità x Impatto Totale**	Definire le azioni migliorative da pianificare per ridurre il livello di rischio.
1) . . . . NAS . .[esempio] . . . . . Il NAS fa da file server, contiene dati personali, è collocato in un armadio chiuso, senza chiave, ha due dischi in RAID 0, sottoposto a backup quotidiano, non viene fatto periodicamente un controllo dello stato di salute dei dischi.	• . . . .Furto	3	R: 5 I: 3 D: 3	TOT = 11	33	- Collocare NAS in un luogo sicuro, chiuso a chiave. - Cifratura dei dati - Backup differenziali in più momenti della giornata
	• . . .Rottura di un disco.	3	R: - I: 4 D: 3	TOT = 7	21	- Collocare NAS in un luogo con condizionamento dell'aria. - Dischi in RAID 1 - Monitoraggio della qualità dei dischi (SMART) - Backup differenziali in più momenti della giornata
	•	. . . .	R: . . . . . I: . . . . . D:	TOT = ...	. . . . .	

2)	•	. . . .	R: . . . . . I: . . . . . D:	TOT = ...	. . . . .	

3. Misure di sicurezza

L'art. 32 del RGPD prevede l'adozione di "*misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*".

L'obiettivo è quello di massimizzare i livelli di Riservatezza, Integrità e Disponibilità delle informazioni, non solo relativamente ai dati personali, ma a tutti i dati che hanno "valore" per l'Organizzazione, abbassando quindi i livelli di rischio legati alle varie minacce e vulnerabilità del sistema.

Le misure di sicurezza devono essere scelte, adottate, implementate e manutenute "*tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*" e vengono suddivise essenzialmente in tre tipologie: misure **tecnologiche** (apparati, software, implementazioni tecnico/informatiche), misure relative alla **sicurezza fisica** (sicurezza di locali, archivi, misure antincendio, antifurto, controlli degli accessi fisici, ecc.), misure **organizzative** (processi e policy interne legate alla gestione della sicurezza).

Le misure di sicurezza si implementano anche attraverso il corretto utilizzo degli strumenti informatici e in generale nella corretta gestione delle informazioni da parte degli utilizzatori. Ulteriori dettagli a questo riguardo verranno definiti e comunicati attraverso lo specifico "Disciplinare sull'uso dei Sistemi Informatici e Informativi" predisposto dai Centri Regolatori/Struttura in accordo con il DPO, come previsto nel Regolamento Nazionale.

3.1. Controllo degli accessi alle risorse informatiche

3.1.1. Procedura di assegnazione delle credenziali di accesso

L'assegnazione di credenziali di accesso alla rete informatica (così come per l'accesso alle aree fisiche riservate) deve essere effettuata a fronte di una richiesta da parte di un responsabile e sulla base di un'esigenza ben definita. In generale i login di accesso sono legati ad un rapporto lavorativo instaurato tra una persona e l'Organizzazione.

Un amministratore di rete autorizzato crea un opportuno login univocamente attribuito al nuovo utente, in base ai criteri stabiliti (preferibilmente nome.cognome, anche per evitare eventuali confusioni in caso di omonimia, soprattutto nell'ambito delle Struttura di più grandi dimensioni) e definisce una password provvisoria, che l'utente dovrà modificare al primo accesso. La password provvisoria viene comunicata direttamente all'utente di persona (previa sua identificazione, se non conosciuto personalmente), a mezzo del telefono (laddove l'amministratore abbia certezza dell'identità dell'utente), oppure mediante invio a mezzo SMS al numero di cellulare, laddove detto numero sia stato previamente certificato come appartenente all'utente.

In caso di cessazione del rapporto di lavoro, deve essere prevista una procedura che, entro un determinato tempo, porti alla disattivazione del relativo account. In questo caso è l'Amministrazione, o chi si occupa del personale, che invierà la richiesta all'area tecnica.

3.1.2. Gestione credenziali con permessi amministrativi

Le credenziali con permessi amministrativi (es. per l'amministrazione di una "Organization Unit" di dominio Windows) devono essere censite e verificate periodicamente.

Le credenziali amministrative non devono essere utilizzate per il normale accesso alle postazioni di lavoro, ma solo per l'accesso a dispositivi di rete a scopo di amministrazione/manutenzione, oppure per l'accesso o esecuzione di specifici applicativi (con l'opzione "esegui come...").

3.1.3. Password policy

La policy generale prevede come requisito minimo le indicazioni previste dalla vecchia normativa privacy, cioè:

- scadenza password ogni 3 mesi;
- lunghezza password di almeno 8 caratteri.

A questi requisiti minimi si suggerisce di aggiungere:

- complessità della password (almeno un carattere maiuscolo, almeno un numero o carattere speciale);
- lunghezza della password di almeno 12 caratteri oppure, in alternativa, sistema di autenticazione a doppio fattore;
- password differente dalle ultime N utilizzate (es. ultime 5);
- blocco dell'account, per un determinato tempo, dopo N tentativi di accesso falliti (es. 5 tentativi), con conseguente necessità di chiedere all'Amministratore la riattivazione dell'account secondo la procedura prevista *sopra* al par. 3.1.1, salvo attendere il tempo necessario per lo sblocco automatico, dove previsto

La password è nota solo all'utente e deve rimanere segreta. Anche gli amministratori di rete non sono a conoscenza delle password utente e possono solo provvedere alla eventuale riassegnazione.

3.1.4. Criteri di accesso alla rete aziendale, agli applicativi e alle risorse di rete

L'account utente, oltre a login e password necessari per l'autenticazione e l'accesso alla rete, comprende anche la definizione dei gruppi di appartenenza dell'utente e di conseguenza i ruoli e i permessi (autorizzazioni) per l'accesso alle risorse.

I permessi che riguardano l'accesso a dati protetti dalla normativa, cioè a tipologie di dati censiti nel Registro dei Trattamenti, devono essere coerenti con le finalità e i limiti di visibilità previsti dai trattamenti stessi.

Le risorse di rete (es. cartella di rete, cloud drive) generalmente richiedono solo l'autenticazione tramite credenziali di rete e i relativi permessi definiti a livello di gruppi.

Alcuni applicativi (ad esempio il Sistema Informativo Nazionale SIN o l'applicazione ConINCA), oltre all'autenticazione tramite login di rete, hanno un sistema interno di profilazione che definisce nel dettaglio ruoli e permessi di utenti/gruppi.

È necessario verificare periodicamente che i permessi di gruppi/utenti per l'accesso alle varie risorse siano coerenti con i relativi ruoli, con le policy aziendali e con le norme privacy relative al trattamento dei dati,

adottando un criterio il più possibile restrittivo, cioè assegnando solo i permessi strettamente necessari. Va adottato quindi il principio di "security by default", per cui un utente, se non espressamente autorizzato, non deve poter accedere ad alcuna risorsa.

3.2. Sicurezza fisica e ambientale

3.2.1. Perimetro di sicurezza fisica, controllo degli accessi all'area di lavoro

L'accesso deve essere consentito solo al personale autorizzato. Per l'accesso da parte di persone esterne (occasionale o continuativo) alle aree di lavoro o alle aree dove risiedono le informazioni, va definita una procedura che consenta di ridurre i rischi (es. identificazione e registrazione degli accessi).

Deve comunque essere ben definito il perimetro dell'area "pubblica" (es. area accoglienza, area di attesa), dove non è richiesta l'identificazione delle persone, dall'area "protetta" (essenzialmente l'area occupata dal personale), dove gli accessi devono essere controllati e le persone identificate.

Nelle aree in cui si svolge un servizio verso utenti esterni, le aree pubblica e protetta possono essere delimitate da uno sportello oppure in alcuni casi da una semplice scrivania: deve però deve essere chiaro il perimetro della zona in cui l'utente può muoversi e quello riservato agli operatori, in cui non può entrare, salvo autorizzazione e identificazione.

I punti di accesso all'area protetta devono essere ben definiti e collocati in posizioni visibili e controllabili (eventualmente tramite videocamera, rispettando le relative norme in materia).

3.2.2. Protezione delle apparecchiature e degli archivi

I dispositivi e i supporti in cui sono conservati i dati, sia digitali che cartacei, devono essere protetti fisicamente da accessi non autorizzati.

In generale le apparecchiature, gli strumenti di controllo dei sistemi e gli archivi fisici, non devono essere collocati nelle aree di accesso al pubblico.

Vanno quindi protetti ad esempio, PC, computer portatili, NAS, hard disk esterni, unità di backup, armadi con documenti, ecc. ma anche apparecchiature di rete come switch, router.

Archivi fisici come armadi o cassettiere, utilizzati per archiviare documenti cartacei, devono essere protetti da accessi non autorizzati (es. chiusura a chiave dell'armadio o del locale, se non presidiato) e da eventi naturali (es. armadi ignifughi). Insieme alla Direzione, si definiscono le regole per la conservazione e utilizzo delle chiavi fisiche, in base alla modalità di utilizzo degli archivi. Una copia delle chiavi andrebbe sempre conservata dalla Direzione in un luogo sicuro (es. in cassaforte).

Le prese di rete, se presenti nelle aree pubbliche, devono essere protette fisicamente, oppure disattivate.

Per tutelare la riservatezza, va definita una collocazione di scrivanie, monitor, area di attesa, archivi, ecc. che non consenta ad un utente di vedere o ascoltare informazioni riguardanti altri utenti. Non vanno quindi lasciati sulla scrivania documenti o faldoni contenenti dati personali che potrebbero essere visti da terzi (policy di "clean desk"), così come dati visualizzati sul monitor del computer.

Nel caso ci sia una sala d'attesa o una fila di persone di fronte ad un operatore, va mantenuta una distanza minima dall'area di lavoro che preservi la riservatezza delle informazioni.

Tutti gli apparati e gli archivi che conservano dati di valore o critici, devono essere protetti da incidenti o furti, eventi naturali (es. allagamenti) e ambientali (es. surriscaldamento), per cui vanno previsti, in base alla valutazione di rischio, gli opportuni impianti antifurto, antincendio, condizionamento, gruppi di continuità, rilevatori di allagamento, ecc.

4. Sicurezza della rete e delle comunicazioni

4.1. Protezione da malware

Su tutte le postazioni utente, deve essere presente un opportuno software antivirus/antimalware costantemente aggiornato.

Per alcune applicazioni particolari, come la posta elettronica, va previsto un sistema di protezione antimalware anche lato server, che filtra eventuali elementi potenzialmente dannosi prima che questi arrivino sulla postazione utente. Anche sugli apparati di rete vanno attivati, dove possibile, le funzionalità di analisi del traffico, blocco di accessi o altri sistemi di protezione (es. sui firewall di ultima generazione).

La protezione da malware implica anche l'aggiornamento puntuale dei sistemi operativi e di altri software eventualmente presenti sulle postazioni utente, dal momento che i malware possono sfruttare vulnerabilità presenti nel sistema.

L'installazione di software sui computer va effettuata solo dal personale tecnico, potendo particolare attenzione all'origine del software e alla sua sicurezza. Gli utenti non devono poter installare software o avere diritti amministrativi sul proprio computer.

La posta elettronica è il principale veicolo di malware ed è spesso l'utente stesso a consentire l'esecuzione di codice malevolo o a fornire informazioni riservate all'esterno, ad es. tramite allegati o meccanismi di fishing. Per questo va prevista un'attività di formazione e responsabilizzazione del personale.

4.2. Piani di backup e procedure di restore di informazioni digitali

Per tutti i dati dell'Organizzazione non già sottoposti a backup a livello centralizzato (gestito dal fornitore di servizio cloud), deve essere definito un opportuno piano di backup, identificando quali dati, con che strumenti e con quale frequenza devono essere effettuati i backup, nonché definita una procedura di restore dei dati, in caso di cancellazione, alterazione, incidente, malfunzionamento o furto dei dispositivi di archiviazione (file server, NAS, ecc.). Vanno definiti i requisiti minimi per la retention dei backup (numero di giorni di conservazione dei backup prima della cancellazione).

Le procedure di backup e restore devono essere documentare e periodicamente testate.

Vanno inoltre definiti i requisiti minimi per i tempi di restore (durata massima accettabile del disservizio) e verificato che gli strumenti e le procedure consentano di rispettare i tempi.

4.3. Sicurezza dell'infrastruttura di rete e dei protocolli di comunicazione

Gli apparati di rete, così come le postazioni utente, devono essere correttamente censiti, configurati e aggiornati.

Va periodicamente effettuata una verifica dei dispositivi connessi alla rete, per assicurarsi che siano tutti tra quelli censiti. In caso contrario va individuato il dispositivo, verificato che la connessione alla rete sia legittima ed eventualmente aggiornato il documento che descrivere gli asset e la relativa valutazione di rischio.

Per i siti web in cui è previsto un meccanismo di autenticazione, oppure contengono dati personali, va adottato sempre un protocollo di comunicazione sicura (HTTPS), con cifratura tramite SSL (TLS).

Per quanto riguarda le reti wi-fi, l'accesso predefinito va effettuato su una rete isolata (guest), in modo che non siano raggiungibili gli altri dispositivi, ma solo la rete internet.

L'accesso a terminal server dall'interno o dall'esterno (via VPN) deve essere effettuata solo tramite algoritmi di cifratura sicuri. Non possono quindi essere utilizzati sistemi operativi obsoleti (es. Windows XP, che non supportano i protocolli più recenti)

L'invio/ricezione della posta elettronica o la comunicazioneattraverso altri sistemi, previa autorizzazione, devono essere effettuati utilizzando protocolli sicuri, con cifratura dei dati (https, cifratura end-to-end, ecc.).

4.1. Controllo sull'invio delle informazioni all'esterno e sicurezza nelle relazioni con i fornitori

L'invio di comunicazioni all'esterno va effettuato tenendo conto del livello di riservatezza con cui l'informazione è stata classificata.

Per informazioni riservate dovranno essere utilizzati canali sicuri di comunicazione e verificato che il destinatario abbia le autorizzazioni per accedere a tali informazioni (in base ai limiti di trattamento definiti per quei dati, descritti nel Registro dei Trattamenti).

Definire in particolare gli strumenti consentiti per l'invio delle informazioni, es. posta aziendale, cloud drive aziendale, ecc. (NO posta personale, cloud di terze parti, ecc.)

Nel rapporto con fornitori esterni, che prevedere lo scambio/condivisione di dati personali/particolari o comunque classificati come riservati, vanno previste apposite clausole di riservatezza.

4.2. Strumenti di monitoraggio e log degli eventi

Per consentire l'individuazione di "non conformità" nell'accesso alle informazioni, vanno predisposti sistemi di monitoraggio o di tracciamento di eventi (log)..
Alcuni eventi che possono essere tracciati sono ad es. login/logout utente, cambio password, accessi negati, blocchi sugli account, ecc.

L’analisi di questi dati consente, ad esempio, di individuare accessi alla rete o a servizi da parte di persone che hanno cessato il rapporto di lavoro con l’Organizzazione, quindi casi di account erroneamente non disattivati e che continuano ad essere utilizzati in maniera illecita.

Per le azioni che coinvolgono utenze amministrative, va fatta un tracciamento mirato (come previsto dal relativo Provvedimento del Garante Privacy del 27/11/2008) ed effettuata periodicamente un'analisi più dettagliata.

Gli strumenti di monitoraggio possono avere anche lo scopo di garantire la continuità operativa dei servizi o degli apparati, notificando eventuali interruzioni e consentendo tempi di interventi il più brevi possibili.

5. Gestione della continuità operativa

Devono essere valutate e documentate le esigenze di continuità operativa dei vari servizi e definite le procedure, i controlli e le migliorie che possono essere implementate per mantenere il livello di continuità richiesto in caso di incidente o condizioni operative avverse.

In fase di valutazione dei rischi, l'esigenza di disponibilità delle informazioni è un aspetto da analizzare strettamente legato alla continuità dei servizi. Se, a titolo di esempio, si danneggia un disco i cui dati sono sottoposti a backup, l'incidente ha impatto sulla disponibilità del dato e questo impatto va valutato per decidere quali azioni prevedere per limitare al massimo il disservizio.

Per questo è necessario prevedere delle procedure di ripristino che non siano limitate ai dati, ma che comprendano tutti gli elementi (server, applicazioni, configurazioni, connettività, ecc) che entrano in gioco nell'erogazione di un servizio.

6. Dismissione o riutilizzo dei supporti di archiviazione dati

6.1. Implementazione di una procedura a norma di legge

Va definire e adottata una procedura per la dismissione/distruzione o il riutilizzo sicuro dei supporti, sulla base delle indicazioni pratiche allegate al Provvedimento del Garante del 13/10/2008 e successive modifiche, integrazioni e/o sostituzioni.

La procedura riguarda anche la distruzione dei documenti cartacei e deve garantire la riservatezza dei dati in tutte le fasi: trasferimento dei supporti o documenti all'interno dell'Organizzazione, trasferimento a fornitore esterno, ecc.

Deve essere mantenuta traccia delle operazioni effettuate sui supporti, sia in caso di distruzione (indicando i dettagli della modalità e tecnica utilizzata) che di riutilizzo (identità dei proprietari, rimozione dei precedenti dati utente, ecc.).

7. Disciplinare sull'uso dei sistemi informatici e informativi

Il Disciplinare sull'uso dei Servizi Informatici e Informativi adottati ai sensi dell'art. 13, comma 5 del Regolamento riassumo le indicazioni operative che gli utenti devono rispettare e costituiscono un importante strumento per aumentare il livello di sicurezza dell'Organizzazione.

Tale documento ha i seguenti obiettivi:

- spiegare sinteticamente e chiaramente le linee guida che l'Organizzazione ha deciso di adottare per limitare i rischi legati all'utilizzo degli strumenti informatici e alle possibili violazioni nel trattamento dei dati. Tutte le indicazioni operative sono un'implementazione delle linee guida generali.
- responsabilizzare e sensibilizzare gli utenti sul tema sicurezza, non solo legata al tema privacy, ma anche per la salvaguardia del patrimonio informativo dell'Organizzazione.
- utilizzo del documento come strumento in fase di formazione (e auto-formazione) del personale e come guida comune a cui fare riferimento;
- informare gli utenti sulle modalità del trattamento dei loro dati personali, ai sensi degli articoli 13 e 14 del RGPD.

Il Centro Confederale Nazionale ha elaborato una bozza del predetto Disciplinare, disponibile nella Intranet sindacale, a cui ciascun Centro Regolatore può fare riferimento, con gli opportuni adattamenti, per la definizione della propria versione.

Si mettono in evidenza di seguito alcuni punti importanti che devono essere trattati nel Regolamento aziendale.

7.1. Postazione di lavoro, password, file server, dispositivi mobili

Non è consentita l'installazione di software senza autorizzazione (per evitare disservizi, minacce di sicurezza, costi di manutenzione).

Linee guida per la scelta di password "robuste", senza pregiudicarne l'usabilità. Segretezza della password.

Non è consentito il salvataggio di dati personali/particolari nel disco locale delle postazioni utente (se non temporaneamente, per esigenze operative). Utilizzare opportune cartelle personali su file server, oppure cloud drive. In caso di necessità di salvare dati in locale, utilizzare opportuni sistemi di cifratura dei dati.

Non salvare dati personali/particolari su supporti rimovibili. Utilizzare eventualmente sistemi di cifratura dei dati.

Non lasciare la postazione di lavoro incustodita. Bloccare il computer nel caso ci si allontani. Non devono essere lasciati incustoditi o visibili a persone non autorizzate eventuali documenti cartacei che l'utente consulta sulla propria postazione di lavoro fisica. Tali documenti devono essere conservati in armadi o cassettiere chiuse a chiave.

La connessione di rete (wifi) per gli smartphone deve essere di tipo "ospiti", cioè non deve consentire di accedere ai dispositivi presenti sulla rete locale. In caso di necessità di accesso a servizi "intranet" attraverso la rete wifi (ad es. da un portatile), va utilizzata una ulteriore modalità di autenticazione e connessione (es. VPN)

In generale non è consentito l'uso di Dispositivi mobili personali (es. PC portatili, palmari, tablet PC) per lo svolgimento e prestazione dell'attività lavorativa, fatti salvi i casi espressamente autorizzati dall'Azienda. In particolare, l'operatore che intenda utilizzare Dispositivi mobili personali per la configurazione della casella di posta aziendale, deve richiedere autorizzazione al proprio Referente. Il Dispositivo mobile deve essere adeguatamente protetto con PIN di sicurezza.

7.2. Attività svolte da remoto

Definire policy di accesso da remoto. Utilizzare, laddove possibile, strumenti aziendali (es. portatile), con accesso via VPN.

In ogni caso la postazione utilizzata dovrà soddisfare dei requisiti minimi di sicurezza e dovrà essere sottoposto a previa verifica da parte dell'Amministratore di Sistema.

In caso di utilizzo di computer personali, se la persona ha anche una postazione fissa in ufficio, accedere via VPN al desktop remoto del computer dell'ufficio (gestendo in maniera opportuna l'accensione/spegnimento del computer).

7.3. Utilizzo della posta elettronica e della rete Internet

Essendo la posta elettronica il principale veicolo di malware e di violazione di dati personali, va posta particolare attenzione alla formazione degli utenti nell'utilizzo di questo strumento e nel riconoscere i potenziali rischi (allegati malevoli, phishing, invio di comunicazioni riservate, ecc.).

Anche l'accesso alla rete Internet e ai relativi servizi esterni deve essere svolto nel rispetto delle linee guida aziendali, evitando quindi il download di materiale non pertinente o pericoloso, la pubblicazione di informazioni via social network, transazioni online, ecc.

7.4. Prolungata assenza e cessazione rapporto di lavoro

Il Disciplinare descrive come può agire l'Organizzazione in caso di prolungata assenza di una persona e necessità di accedere urgentemente a dati protetti dall'account utente (es. cartella personale, casella di posta).

In caso di cessazione del rapporto di lavoro, deve essere definita la procedura di disattivazione dei servizi dell'utente, restituzione dei dispositivi aziendali, disattivazione di login e email.