OpNet S.r.l.
Sede Legale Via Monte Rosa, 91 - 20149 Milano (MI)
Tel 06 52 09 70 01 **PEC** pec.opnet@legalmail.it
opnet.it
CF/P.IVA 17502511003 **REA** MI-2738750
Capitale sociale **EUR € 20.000,00** interamente versato

ISTRUZIONI OPERATIVE PER LE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI CON ACCESSO ALLA PIATTAFORMA PER LE SEGNALAZIONI WHISTLEBLOWING DI OPNET

CONTESTO DI RIFERIMENTO

Il Regolamento UE n. 679/2016 (di seguito GDPR) e la normativa italiana di riferimento e successive modificazioni e integrazioni, impone all'Azienda di trattare con particolare cura i dati personali dei soggetti con cui entra in contatto, siano essi dipendenti, fornitori di beni e servizi, clienti, consulenti, etc. Ai sensi dell'art. 2-*quaterdecies* del D.lgs. 196/2003 (Attribuzione di funzioni e compiti a soggetti designati) introdotto dal D.lgs. 101/2018, il titolare ha previsto, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità nonché a persone che lui stesso ha provveduto ad autorizzare al trattamento dei dati personali nei limiti e nel rispetto del GDPR e del sopra citato decreto. Tutti coloro che trattano dati personali nello svolgimento della propria attività lavorativa sono designati quali Persone autorizzate al trattamento dei dati.

La presente opera quale ulteriore specifica rispetto alla nomina già in essere, ad incaricato al trattamento e relative istruzioni allegate all'informativa sul trattamento di dati personali in relazione al rapporto con te intercorrente, per quanto riguarda le attività di trattamento di dati in relazione alla gestione delle segnalazioni di violazioni ("Segnalazioni Whistleblowing") ai sensi del d.lgs. 24/2023 ("Decreto") e "Altre Segnalazioni" ai sensi delle Politiche che regolano il Whistleblowing per la società OpNet s.r.l. di seguito OpNet

La specificità dei trattamenti dati personali connessi alla gestione delle Segnalazioni Whistleblowing richiede una particolare attenzione affinché detti trattamenti avvengano nel pieno rispetto della normativa privacy di volta in volta applicabile, ivi incluse le istruzioni di cui alla presente nomina ad incaricato

OpNet quindi, come titolare del trattamento, è tenuta ad impartire le seguenti Istruzioni Operative, che dovrai seguire in qualità di persona autorizzata al trattamento dei dati personali dei Clienti/Fornitori/Prospect/Dipendenti/Soggetti terzi (es: Istituzioni, dealer) connessi alla gestione delle Segnalazioni Whistleblowing alle condizioni e nei limiti indicati nella presente nomina.

Tali istruzioni operative dovranno essere rispettate anche nel compimento delle attività operative di trattamento dei dati personali il cui Titolare/Responsabile è la società WindTre S.p.A. e per le quali sei stato autorizzato al trattamento, come dipendente di OpNet.

In qualità di Persona autorizzata sei chiamato ad operare mediante l'utilizzo di mezzi elettronici o automatizzati sotto la diretta autorità del Titolare eseguendo le istruzioni impartite dallo stesso e/o

contenute all'interno delle presenti Istruzioni Operative per la Persona autorizzata e di seguito meglio specificate.

Ti ricordiamo che la piattaforma whistleblowing è uno strumento sicuro e riservato per segnalare comportamenti illeciti o contrari all'etica aziendale, nel rispetto della normativa sulla protezione dei dati personali (es. GDPR, D.Lgs. 24/2023).

- I dati raccolti sono trattati in conformità al GDPR e alle normative nazionali.
- Le segnalazioni sono archiviate in ambienti digitali criptati e protetti.
- Solo il personale autorizzato può accedere alle segnalazioni, nel rispetto del principio di necessità e proporzionalità.

In qualità di persona autorizzata al trattamento dei dati personali, limitatamente alle attività di gestione delle segnalazioni whistleblowing della società di Opnet, sei autorizzato a trattare i dati personali contenuti nelle segnalazioni whistleblowing esclusivamente per le seguenti finalità:

- ricezione, registrazione e valutazione delle segnalazioni;
- gestione delle indagini interne;
- comunicazioni con il segnalante (se identificato);
- archiviazione e conservazione dei dati secondo i termini previsti.

E ti impegni a:

- trattare i dati nel rispetto delle istruzioni ricevute dal Titolare;
- rispettare le vigenti misure di protezione e sicurezza, così come indicate nelle policy e procedure aziendali relativamente al trattamento dei dati personali e pubblicate sulla intranet aziendale nella specifica sezione "Whistleblowing";
- garantire la riservatezza e la sicurezza dei dati;
- non divulgare, copiare o utilizzare i dati per finalità diverse da quelle indicate;
- segnalare immediatamente al Titolare eventuali violazioni o incidenti di sicurezza;
- accedere ai dati solo se strettamente necessario per lo svolgimento delle mansioni.

Potrai avere visione delle segnalazioni riferite alla società indicata nella specifica nomina.

Inoltre, ti ricordiamo che è tua responsabilità, altresì, osservare ulteriori accorgimenti. In particolare:

• dovrai attenerti a quanto previsto dalle procedure emesse al fine di fornire indicazioni ed istruzioni sulle modalità operative e sui comportamenti da tenere nello svolgimento delle tue attività all'interno della funzione di appartenenza;

• tutti i dati devono essere trattati per le finalità per le quali sono stati raccolti e per il tempo necessario allo svolgimento delle attività;

• la raccolta, l'organizzazione e la conservazione dei dati deve essere gestita con particolare attenzione affinché nessuno lasci documenti in luoghi facilmente accessibili (stampanti, fax, cestini, etc.);

• in generale tutta la documentazione ed in particolare quella contenente dati giudiziari, dovrà essere sempre conservata negli appositi armadi/classificatori presenti nei locali della Direzione;

• il trasferimento di informazioni ad eventuali strutture esterne dovrà essere effettuato solo se strettamente necessario ai fini dei trattamenti previsti e secondo quanto stabilito dalle Procedure aziendali;

• in generale l'accesso alle informazioni ed ai sistemi dedicati alla fornitura dei servizi tipici della funzione di appartenenza (sia elettroniche che cartacee) deve essere limitato alle sole persone che siano appartenenti alla funzione oppure soggetti terzi preventivamente autorizzati.

Ai sensi delle norme di sicurezza, per una corretta analisi degli incidenti informatici e visti gli obblighi richiamati dalle norme sul data breach (art. 33 del GDPR), ti chiediamo di segnalare tempestivamente al tuo superiore diretto eventuali situazioni di rischio per la sicurezza dei dati di cui hai avuto evidenza (es. la violazione della password, il tentativo di accesso non autorizzato ai sistemi) ovvero che riguardino i soggetti esterni autorizzati all'accesso (palesi violazioni delle procedure aziendali): la tua collaborazione è importante al fine di colmare eventuali lacune nei sistemi di sicurezza e nelle procedure relative alla tutela dei dati personali trattati. Ti ricordiamo infine che l'utilizzo per scopi personali o comunque per fini non legittimi dei dati ai quali hai accesso o hai acceduto, anche nel caso in cui non dia origine ad un danno e/o ad una responsabilità in capo a Wind Tre secondo la legge italiana, potrebbe comunque comportare l'applicazione di sanzioni disciplinari, potendosi configurare quali violazioni ai doveri che incombono sul dipendente, così come previsti dal CCNL/TLC ad oggi vigente.

SCOPO E CAMPO DI APPLICAZIONE DELLE ISTRUZIONI OPERATIVE

Ai sensi delle finalità e degli obblighi del GDPR nonché dell'art. 2-*quaterdecies* del D. Lgs.196/2003 (di seguito anche Codice privacy) forniamo le presenti istruzioni al personale autorizzato al trattamento dei dati personali nell'ambito attività relative alla gestione delle segnalazioni Whistleblowing.

PANORAMICA SUI PRINCIPALI RIFERIMENTI NORMATIVI APPLICABILI

Ai sensi dell'art. 2 del D.lgs. 24/2023 si intende per:

- "**Violazioni**": comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato (art. 2, comma 1, lettera a)
- "**Segnalazione**": la comunicazione scritta o orale di informazioni sulle violazioni (art. 2, comma 1, lettera b);

- "**Persona Segnalante**" (o anche solo "Segnalante"): la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo (art. 2, comma 1, lettera d);
- "**Persona Coinvolta**": la persona fisica o giuridica menzionata nella segnalazione ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente (art. 2, comma 1, lettera e);
- "**Seguito**": l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate (art. 2, comma 1, lettera f).

Ai fini della normativa privacy, si intende per:

a) "trattamento", qualunque operazione o complesso di operazioni, svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati (art. 4. punto 2 del GDPR);

b) "dato personale", qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (art. 4 punto 1 del GDPR);

c) "dati sensibili" (dati particolari), qualunque dato personale idoneo a rivelare "l'origine razziale od etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale" (art. 4 punto 15 relativamente ai dati idonei a rivelare lo stato di salute, art. 9 GDPR per tutti gli altri);

d) "dati giudiziari" (art. 10 del GDPR), i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale. Ai sensi delle nuove norme introdotte nel Codice privacy, dal D. Lgs.101/2018, si tengano presenti anche gli artt. 2-*octies*, comma 3 lett. e) (Principi relativi al trattamento di dati relativi a condanne penali e reati), art. 2 -*undecies* (Limitazioni ai diritti dell'interessato), comma 2 lett. e) nonché dall' art. 2-*duodecies* (Limitazioni per ragioni di giustizia) in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia e alle eventuali limitazioni previste dalla legge in caso di esercizio dell'interessato dei diritti e degli obblighi di cui agli articoli da 12 a 22 e 34 del GDPR nonché delle altre limitazioni previste per tutte le altre ragioni di giustizia indicate dalla legge.

Il GDPR ai sensi dell'art. 5 (Principi applicabili al trattamento di dati personali) richiede che i dati siano utilizzati secondo i principi di seguito elencati. In particolare, essi devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

La legge identifica le figure che, a diversi livelli di responsabilità, devono rendere conto della corretta gestione dei dati personali:

- il Titolare, rappresentato dalla persona fisica o giuridica cui competono le decisioni circa le finalità e le modalità di trattamento di dati personali, ivi compresa la sicurezza dei dati;
- la persona espressamente Designata ossia la persona fisica che opera sotto l'autorità del Titolare e a cui quest'ultimo ha attribuito specifici compiti e funzione connesse al trattamento dei dati personali, ai sensi dell'art. 2-quaterdecies del Codice privacy. Wind Tre nell'ambito della figura espressamente designata così come sopra definita, ha fatto rientrare la figura del Designato del trattamento (denominato ex tunc "Responsabile interno") che ha ricevuto una specifica nomina firmata per accettazione e della Persona autorizzata (denominato ex tunc 4 "Incaricato del trattamento") che ha ricevuto le presenti istruzioni operative mediante pubblicazione sulla intranet aziendale;
- il Responsabile (denominato ex tunc "Responsabile esterno") ossia la persona fisica o giuridica che tratta dati per conto del Titolare del trattamento ai sensi dell'art 28 GDPR

ISTRUZIONI OPERATIVE DA SEGUIRE IN QUALITA' DI PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI

In base all'art. 32 del GDPR (disciplinato in precedenza all'articolo 31 del Codice privacy) stabilisce che i dati debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento (nominato ai sensi dell'art 28 del GDPR) devono mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio. Di seguito s'illustrano le istruzioni comportamentali e tecniche che in qualità di persona autorizzata devi seguire nello svolgimento delle tue attività lavorative fermo restando che maggiori dettagli tecnici, organizzativi e procedurali sono contenute nelle specifiche

policy, procedure, codici di condotta pubblicati nella intranet aziendale a cui si rimanda integralmente. Per eventuali chiarimenti potrai far riferimento alla Direzione Regulatory Affairs Wind3, funzione Privacy Regulations Wind3, scrivendo alla e-mail affariregolamentari_privacy@windtre.it

Le regole di ordinaria diligenza

Nell'esecuzione dei compiti assegnati, devi attenerti ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento. Gli obblighi di ordinaria diligenza sono peraltro sanciti dall'art. 1176 del codice civile, il quale precisa come "Nell'adempimento delle obbligazioni inerenti all'esercizio di un'attività professionale, la diligenza deve valutarsi con riguardo alla natura dell'attività esercitata".

Per queste ragioni, nello svolgimento delle mansioni che ti sono state affidate devi prestare particolare attenzione nel:

▪ non divulgare a terzi estranei le informazioni di cui viene a conoscenza;

▪ non condividere, comunicare o inviare, in qualsiasi forma, a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative i dati e/o informazioni;

▪ non fare copie, per uso personale, dei dati su cui svolgono operazioni;

▪ attenersi scrupolosamente alle presenti istruzioni scritte.

Oltre alle suindicate regole generali se ne aggiungono altre. In caso di abbandono temporaneo (anche per breve tempo) della propria postazione di lavoro, è necessario provvedere a:

• raccogliere la documentazione cartacea contenente dati personali in modo da non lasciarla alla visuale di eventuali soggetti che si trovano a transitare nei pressi della postazione di lavoro;

• chiudere gli eventuali file contenenti dati personali I dati particolari (sensibili) devono essere trattati in modo conforme all'art. 2-sexies (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante) comma 1, 2 lett dd e comma 3 del Codice privacy, nonché all'art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute) commi 7 e 8 del Codice privacy e per i dati relativi alla salute anche tenendo conto delle misure di garanzia stabilite con il provvedimento biennale del Garante privacy di cui all'art. 2-septies commi 2 e 5 del Codice privacy.

L'accesso ai dati dalla postazione di lavoro

Per lo svolgimento della tua attività si deve poter accedere da una postazione di lavoro. Se da questa si accedono a dati personali, conservati in formato elettronico, devi adottare le seguenti cautele:

▪ utilizzare una password sia all'accensione sia nel caso d'accesso alle risorse di rete insieme alla propria user-id;

▪ utilizzare, dove richiesto, user-id e password per l'accesso all'applicazione attraverso la quale si accede ai dati;

▪ chiudere le applicazioni in uso prima di allontanarsi dalla postazione di lavoro anche per brevi periodi;

▪ impostare uno screen saver con password in modo che si attivi dopo 15 minuti di inattività in caso di allontanamento temporaneo dalla propria postazione di lavoro inibendo la vista ad altri soggetti. In caso di impossibilità, utilizzare la combinazione CTRL+ALT+CANC (o Win+L) per bloccare la postazione;

▪ non scaricare dati personali se non strettamente necessari alle attività delle proprie mansioni seguendo le istruzioni del Designato

La gestione delle password per l'accesso ai sistemi

Per una corretta gestione delle password, devi avere cura di:

▪ modificare la password al primo accesso successivo all'assegnazione, avendo cura di impostare la password con una lunghezza di almeno 10 caratteri (dove non previsto diversamente) e secondo le caratteristiche che sono state previste (ad es. uso di caratteri speciali come !@%*&^$#...; uso di lettere minuscole e maiuscole, numeri);

▪ la password non deve contenere sequenze di tre o più caratteri identici;

▪ evitare di rimettere le ultime 10 password utilizzate;

▪ non è consentito l'uso di password di default;

▪ non è consentito l'uso di password predefinite;

▪ mantenere la password riservata e non divulgarla a terzi, anche se persone autorizzate del trattamento;

▪ non trascriverla su fogli, agendine, post-it facilmente accessibili a terzi o su altro supporto informatico (ad es. codice software) a meno che non si provveda d un'adeguata protezione della stessa (ad es. encryption);

▪ non è consentita la conservazione di file contenenti elenchi di password;

▪ non utilizzare parole del dizionario;

▪ laddove per la password non sia prevista una scadenza da parte del sistema stesso, provvedere alla sua sostituzione almeno ogni due mesi o quando viene meno la loro caratteristica di riservatezza;

▪ non basarla su informazioni facilmente deducibili quali ad es. il nome proprio o di parenti, la data di nascita, il proprio codice fiscale;

▪ non sono ammesse password uguali alla corrispondente user-id (identificativo utente);

▪ non includere la password in alcun processo di connessione automatica (ad es. tasi funzione, macro, etc);

▪ utilizzare per l'accesso ai sistemi identificati una password differente rispetto a quella utilizzata per accedere ai diversi sistemi/applicazioni se di differente livello di sicurezza;

▪ utilizzare in ambito aziendale una password che non corrisponde a servizi/siti Internet personali;

▪ utilizzare una password diversa da quelle utilizzate in passato almeno negli ultimi180 giorni.

Nel caso in cui una password perda di segretezza (ad es. per l'accidentale smarrimento della stessa, la divulgazione a terzi per motivi di lavoro, etc.), previa comunicazione al tuo diretto responsabile, devi provvedere alla sua immediata sostituzione.

È opportuno sapere che:

▪ in caso di mancato utilizzo, per un periodo superiore a sei mesi la user-id potrà essere disabilitata;

▪ in caso di revoca/esclusione dall'incarico che consentiva l'accesso all'elaboratore o all'applicazione, la user-id viene a decadere con decorrenza immediata.

Qualora, in relazione alle caratteristiche dell'elaboratore e/o dei sistemi e/o delle applicazioni accedute, non fosse possibile seguire uno o più adempimenti sopra indicati per la corretta gestione della password, devi comunicare tale circostanza al tuo diretto responsabile, il quale attiverà le eventuali ed opportune procedure di escalation verso il responsabile preposto per grado che identificherà le azioni correttive per il corretto recepimento degli adempimenti. In ogni caso, con tale comunicazione si ritiene che tu abbia assolto ai tuoi doveri e potrai continuare ad operare secondo consuetudine, salvo diverse disposizioni scritte da parte del responsabile preposto per grado nei confronti del tuo responsabile diretto che provvederà ad inviartele.

Utilizzo e custodia di strumenti per l'autenticazione

È possibile che in alcuni casi per l'accesso a postazioni di lavoro o a sistemi/applicazioni tu venga dotato di dispositivi di autenticazione supplementari (ad es.: Smart Card, Token per la generazione di "On Time Password"; Token\altri strumenti per la rilevazione delle caratteristiche biometriche…) Si ricorda che questi strumenti forniscono credenziali di autenticazione e che ti sono stati assegnati in modo riservato.

Come tali:

▪ devi custodirli con perizia non consegnandoli a nessuno, nemmeno ad altre Persone autorizzate al trattamento;

▪ non devono essere lasciati incustoditi;

▪ non devono essere comunicate le caratteristiche, né codici identificativi o numeri seriali, o quant'altro che possa consentire a chiunque una precisa identificazione;

▪ la "one time password" generata da o con questi strumenti non deve essere fornita a nessuno per nessuna ragione;

▪ nell'effettuare l'accesso alla postazione o al sistema con le proprie credenziali, non si deve consentire che attraverso queste credenziali un altro soggetto, anche se persona autorizzata al trattamento, possa effettuare operazioni.

In caso di perdita del possesso, anche temporaneo, sei tenuto ad informare immediatamente il tuo diretto responsabile che provvederà a far disattivare/invalidare le credenziali di autenticazione fornite dallo strumento. In mancanza di tale segnalazione, eventuali usi indebiti verranno univocamente associati al titolare del token stesso.

L'uso dell'antivirus e altri accorgimenti

Per minimizzare i danni che possono essere causati dai virus informatici, Wind Tre gestisce tre aspetti:

▪ le politiche di prevenzione per impedire l'introduzione dei virus all'interno dell'azienda;

▪ le politiche per la rilevazione della presenza dei virus all'interno di applicazioni, dati o boot record;

▪ le politiche di rimozione di eventuali virus presenti.

In ogni caso, sei tenuto a rispettare alcuni principi di base, quali:

▪ evitare di introdurre applicazioni/software senza una approvazione da parte del tuo diretto responsabile;

▪ controllare che il programma antivirus installato sia sempre funzionante;

▪ verificare, con l'ausilio del programma antivirus in dotazione, ogni supporto per lo storage di dati (, chiavi USB, unità disco esterne, memorie flash), prima dell'esecuzione dei file in esso contenuti, laddove questo non sia attivato automaticamente;

▪ prestare sempre debita attenzione agli eventuali messaggi di segnalazione di virus e, in caso di anomalie, contattare immediatamente il tuo diretto responsabile e/o le unità tecniche aziendalmente preposte;

▪ evitare di rispondere a mail che richiedono una conferma di lettura (se non da account conosciuti) o che invitano a cancellarsi da mailing list;

▪ segnalare tempestivamente al proprio diretto responsabile e/o alle unità tecniche aziendalmente preposte i casi di spamming o comunque di ricevimento non richiesto di mail a sfondo commerciale, sessuale o finanziario;

▪ non partecipare né contribuire a diffondere mail il cui testo contiene inviti alla spedizione del messaggio a quanti più utenti possibile;

▪ non trattare dati eccedenti rispetto alle tue mansioni e comunque sempre pertinenti e proporzionati alla finalità per la quale hai necessità di trattarli, fermo retando il rispetto delle misure di sicurezza aziendali.

È altresì buona norma disabilitare le opzioni presenti su alcuni tool come Outlook della Microsoft, che di default aprono il messaggio a prescindere dalla volontà del ricevente.

Le modalità per il salvataggio dei dati

L'utilizzo del disco locale (C:\ - D:\ ...) del proprio computer per mantenere copie di tabelle, fogli Excel, documenti word contenenti dati personali e/o informazioni riservate quali indirizzi, numeri telefonici,

anagrafiche di clienti, fornitori o dipendenti al termine della giornata lavorativa è fortemente sconsigliato ancorché non proibito in via generale salvo differenti disposizioni dei propri Responsabili (diretto o per grado). Nel caso in cui sia necessario utilizzare supporti removibili per la memorizzazione temporanea di dati personali (ad es. per la copia e lo scambio di informazioni), devi osservare alcune precauzioni al fine di salvaguardare la riservatezza degli stessi. In particolare, devi:

▪ utilizzare i supporti solo dopo aver provveduto a cancellare i dati e le informazioni precedentemente contenuti;

▪ evitare di lasciare incustoditi i supporti di memorizzazione;

▪ provvedere all'"encrypting" dei dati memorizzati sul supporto comunicando la password di "encryption" solo al destinatario dei suddetti dati memorizzati;

▪ non condividere i supporti di memorizzazione con altri colleghi.

In generale l'uso di qualsiasi tipo di supporto per memorizzare i dati personali è fortemente sconsigliato e nel caso di necessità è opportuno inviare una richiesta di autorizzazione al tuo diretto responsabile.

Archivi su supporti cartacei

Tutti i dati personali presenti su supporti di tipo cartaceo devono essere riposti in archivi mantenuti chiusi e dislocati all'interno di locali ad accesso controllato e limitato. Puoi accedere ai soli archivi di tua competenza (ad es. solo quelli relativi all'area organizzativa di appartenenza) e devi adottare le seguenti precauzioni:

▪ l'accesso è permesso per il tempo necessario allo svolgimento delle proprie mansioni;

▪ la documentazione eventualmente prelevata deve essere riposta negli archivi al termine delle operazioni di trattamento. Durante la consultazione giornaliera, la Persona autorizzata avrà cura di tenerli sul proprio tavolo in maniera tale da non rendere visibile il contenuto a terzi;

▪ in ogni caso tutti i documenti contenenti dati sensibili utilizzati nello svolgimento delle proprie mansioni quotidiane, devono essere riposti, a fine giornata, in contenitori preferibilmente muniti di serratura (ad es. cassettiere, armadi);

▪ qualora si acceda ad un locale esplicitamente dedicato ad archivio al di fuori dell'orario di lavoro canonico (ad es. prima delle 8 e dopo le 18), è necessario informare il diretto responsabile.

Mezzi di trasmissione e riproduzione dei documenti

Nell'utilizzo di fax, stampanti, fotocopiatrici è importante adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di altre persone non autorizzate a prendere visione del contenuto. A tal fine devi:

▪ utilizzare sempre le procedure di secure printing ed evitare di lasciare incustoditi presso il fax, la stampante di rete o la macchina fotocopiatrice documenti contenenti dati personali;

▪ accertarsi in caso di uso della fotocopiatrice che non rimangano originali o copie nella macchina. In caso di cattiva qualità della stampa distruggere il supporto cartaceo e non riutilizzarlo come carta da riciclo;

▪ nel caso di trasmissione via fax di documenti contenenti dati personali, accertarsi telefonicamente dell'avvenuta ricezione e prestare la massima attenzione all'effettiva identità del destinatario. Una volta inviati i documenti, ritirarli immediatamente dalla macchina.

GESTIONE DELLE AUTORIZZAZIONI ALL'ACCESSO DELLE RISORSE INFORMATICHE

Nel caso di trattamento di dati personali effettuato mediante l'ausilio di strumenti elettronici, è prevista l'adozione di un sistema di autorizzazioni all'accesso alle risorse informatiche.

I profili di autorizzazione, per ciascuna Persona autorizzata o per classi omogenee di persone autorizzate, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Le autorizzazioni devono avere ad oggetto i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione e devono essere rilasciate e controllate dal diretto responsabile. Quest'ultimo, almeno una volta l'anno, deve verificare la sussistenza delle condizioni per il loro mantenimento in essere anche con l'ausilio dell'Ufficio Privacy attraverso una valutazione d'impatto (DPIA) ai sensi dell'art. 35 del GDPR.

Assegnazione/revoca/sospensione del profilo

L'assegnazione di un nuovo profilo deve, a livello generale, conformarsi ai seguenti principi:

▪ autorizzare le Persone autorizzate all'accesso ai dati personali/particolari, la cui conoscenza sia necessaria per lo svolgimento delle operazioni di trattamento, in relazione alla nomina attribuita nonché al ruolo e alla mansione ricoperta;

▪ nel richiedere l'abilitazione all'accesso, i richiedenti devono sempre ispirarsi ai principi di "accesso sulla base della effettiva necessità di conoscere" e di "accesso con il minimo privilegio operativo necessario";

▪ le autorizzazioni vanno gestite anche in caso di revoca per dimissioni o sospensione temporanea dall'incarico.

Nel caso di assenza prolungata dal lavoro da parte della Persona autorizzata (ad esempio per maternità, seri motivi di salute, aspettative e, comunque, per periodi superiori a tre mesi) sarà cura del Designato del trattamento e/o di apposite strutture demandate a tale compito dal Designato o aziendalmente preposte, disabilitare (anche temporaneamente) il profilo di accesso specificando la data effettiva a partire dalla quale il profilo sarà disabilitato.

È di competenza del Designato del trattamento e/o di apposite strutture demandate a tale compito dal Designato che comunque operano sotto la sua diretta responsabilità o aziendalmente preposte anche la revoca del profilo in caso di dimissioni o di cambio di ruolo del dipendente.

Altre misure

Accesso a dati personali, banche dati ed applicazioni aziendali: i dati, le banche dati e le applicazioni aziendali cui potrai accedere sono quelli strettamente indispensabili per l'esecuzione della tua prestazione, in linea con le responsabilità e, per quanto attiene alle applicazioni informatiche, secondo il profilo di utenza che ti è stato assegnato. Tutte le variazioni ti verranno comunicate di volta in volta da chi di competenza.

Creazione di nuove applicazioni: senza essere stato preventivamente autorizzato, non dovrai di tua iniziativa attivare nuove procedure informatiche per la gestione o elaborazione di dati, archivi anche cartacei o files di persone, fisiche o giuridiche. Qualora ciò si rendesse necessario, dovrai darne preventiva comunicazione al tuo superiore diretto e procedere solo dopo aver ricevuto formale autorizzazione.

Comunicazione e diffusione: i dati cui hai accesso nel corso dell'attività lavorativa dovranno essere trattati da te personalmente mentre non potranno essere trasmessi a terzi, esterni all'azienda, se non espressamente previsto dalle procedure aziendali, dalla normale prassi o richiesto dalla propria attività.

Richieste di accesso / esercizio dei diritti: qualora ricevessi una richiesta di accesso ai propri dati da parte di un soggetto interessato (sia esso un dipendente dell'azienda, un fornitore, un cliente, un consulente, etc.), ne dovrai prendere nota scritta, annotando la data e i dati anagrafici del soggetto interessato, dandone poi immediatamente notizia al tuo diretto superiore.

Altre Misure di sicurezza

➢ Ti chiediamo di segnalare tempestivamente al tuo superiore diretto eventuali situazioni di rischio per la sicurezza dei dati di cui hai avuto evidenza (es. la violazione della password, il tentativo di accesso non autorizzato ai sistemi, etc.), ovvero che riguardino i soggetti esterni autorizzati all'accesso (es. palesi violazioni delle Procedure aziendali). La tua collaborazione è importante al fine di colmare eventuali lacune nei sistemi di sicurezza e nelle procedure relative alla tutela dei dati personali trattati

➢ Deve essere posta molta attenzione nella gestione di materiale contenente dati di rilevanza sensibile o giudiziaria. Per una migliore guida in materia di sicurezza, sei comunque invitato a seguire le Policies aziendali.

➢ La raccolta, l'organizzazione e la conservazione dei dati deve essere gestita con particolare attenzione affinché nessuno lasci documenti in luoghi facilmente accessibili (stampanti, fax, cestini, etc).

➢ Il trasferimento di informazioni ad eventuali strutture esterne dovrà essere effettuato solo se strettamente necessario ai fini dei trattamenti previsti e secondo quanto stabilito dalle Procedure aziendali.

Qualora tu sia stato designato "Amministratore di sistema", in ottemperanza a quanto disposto nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, così come modificato dal successivo Provvedimento del 25 giugno 2009, dovrai, altresì, attenerti alle Istruzioni riguardanti gli ambiti

di operatività consentiti in base al profilo di autorizzazione assegnato ed allegate alla specifica lettera di nomina per tale incarico.

Si ricorda che l'utilizzo per scopi personali o comunque per fini non legittimi dei dati ai quali hai accesso o hai acceduto, anche nel caso in cui non dia origine ad un danno e/o ad una responsabilità in capo a Wind Tre. secondo la legge italiana, potrebbe comunque comportare l'applicazione di sanzioni disciplinari, potendosi configurare quale violazione ai doveri che incombono sul dipendente, così come previsti dal CCNL applicabile, ed eventualmente anche penali. Il GDPR prevede, per chi lo disattende, sanzioni civili e penali, ma anche provvedimenti da parte dell'Autorità Garante che, ove ravvisasse ipotesi di trattamenti illeciti o non conformi ovvero mere violazioni delle disposizioni normative può disporre ispezioni di verifica ed imporre anche il blocco dei trattamenti. Ai sensi degli artt. 167 e ss del Codice privacy è vietato e sanzionato con la pena della reclusione il trattamento illecito dei dati personali in violazione delle norme sui dati relativi al traffico (art. 123), all' ubicazione (art.126) e alle chiamate indesiderate (art. 130); il trattamento illecito dei sensibili (particolari) o giudiziari, nonché la comunicazione e la diffusione illecita di dati personali in violazione degli articoli 2-ter, 2-sexies e 2- octies del Codice privacy (o comunque in tutti i casi se la diffusione avviene senza consenso) se la violazione ha ad oggetto un archivio o di parte sostanziale di esso e sempre che tali dati personali siano per loro natura oggetto di trattamento su larga scala. È punito inoltre chiunque acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala [1]

Le suddette istruzioni operative valgono e sono efficaci anche nel caso in cui le attività di trattamento riguardano dati per cui OpNet è nominata, ai sensi dell'art. 28 del GDPR, "*Responsabile esterno del trattamento*"

---

[1] **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