Tutela della privacy

"Regolamento Europeo"
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679

Registro del trattamento

Dr. Davide Candia

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Accountability e approccio basato sul rischio

Il GDPR non ha solo ampliato i diritti riconosciuti all'interessato, ma si è concentrato sulla maggiore responsabilizzazione dei soggetti coinvolti nel trattamento dei dati personali, mostrando grande interesse al tema della data security.

Il GDPR adotta taluni "strumenti" al fine di rafforzare la tutela dei dati e la responsabilizzazione del Titolare e del Responsabile del trattamento:

- sancisce il principio di *accountability* (Art. 5, par. 2);
- sancisce i principi della *privacy by design* e della *privacy by default*;
- Prevede la tenuta **del Registro dei trattamenti;**
- richiede d'implementare adeguate misure di sicurezza, tenendo in considerazione le tipologie di operazioni svolte e i relativi livelli di rischio, affinché non si verifichino violazioni dei dati;
- introduce la figura del **Data Protection Officer**.

Il principio di *accountability* ambisce a realizzare il passaggio da una concezione di adempimento formale della normativa privacy, ad un approccio sostanziale di protezione dei dati, connesso alla natura delle attività concretamente svolte, all'analisi dei rischi e alle misure di sicurezza che risultino adeguate alle singole fattispecie.

Registro delle attività di trattamento - Art. 30

Il Registro delle Attività di Trattamento (**PRIVACY BOOKING**) sarà un documento di tipo dinamico ed una sorta di memoria storica dell'azienda in materia di sicurezza dei Dati.

Nome e contatti di ogni Responsabile (esterni e interni)

Finalità di Trattamento (motivo del Trattamento)

Categorie di Interessati e di Dati trattati

Categorie di destinatari a cui i dati sono comunicati

Informazioni sui trasferimenti verso paesi terzi

Termini per la cancellazione dei dati

Misure di sicurezza tecniche e organizzative

Backup & Recovery

Reg. Informatico

Policy e Procedure

Formazione

Registro delle attività di trattamento – Art. 30

Gli obblighi di cui all'Art.30 non si applicano alle aziende con meno di **250 dipendenti**, tranne nei seguenti casi:

Trattamento con rischi per diritti e libertà dell'Interessato

Trattamento non occasionale dei dati

Trattamento di categorie particolari di dati

Trattamento di dati relativi a condanne penali e reati

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Trattamento dati: rischi per gli interessati

- I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo

TRATTAMENTO NON OCCASIONALI
parere EDPB *European Data Protection Board*

- Per rientrare nella casistica del trattamento non occasionale è sufficiente eseguire un trattamento in modo *permanente* e *continuativo* come ad esempio una **piccola azienda** che tratta regolarmente i **dati** dei **dipendenti** che, in qualche modo, contengono sempre *dati sensibili* per esempio nei cedolini o nelle cartelle mediche di idoneità.
- Altri casi di *"trattamento non occasionale"*, potrebbero essere quelli di un **professionista** che tratta i dati **per conto** dei clienti in qualità di **responsabile** o un **sito web** che raccolga i dati attraverso una normalissima form di richiesta informazioni.
- I casi più comuni sono quelli del *Medico del Lavoro*, il *Consulente Paghe, il Fiscalista* o la *Web Agency* che gestisce il sito web piuttosto che l'azienda che fa *Assistenza IT* riportati anche nell'elenco sotto.

Articolo 30
Registri delle attività di trattamento

3. I registri di cui ai paragrafi 1 e 2 sono tenuti in **forma scritta, anche in formato elettronico.**

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento **mettono il registro a disposizione dell'autorità di controllo.**

Alla luce di quanto detto, sono tenuti all'obbligo di redazione del registro:

- PPAA- OSPEDALI-CLINICHE, LABORATORI,
- Esercizi commerciali, esercizi pubblici o artigiani con almeno un dipendente (bar, ristoranti, officine, negozi, piccola distribuzione, ecc.)e/o che trattino dati sanitari dei clienti (es. parrucchieri, estetisti, ottici, odontotecnici, tatuatori ecc.);
- Liberi professionisti con almeno un dipendente e/o che trattino dati sanitari e/o dati relativi a condanne penali o reati (es. **commercialisti, notai, avvocati, osteopati, fisioterapisti, farmacisti, medici in generale**);
- Al di fuori dei casi di tenuta obbligatoria del Registro, anche alla luce del considerando 82 del GDPR**, il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento**, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce a meglio attuare, con modalità semplici e accessibili a tutti, **il principio di accountability** e, al contempo, ad **agevolare in** maniera dialogante e collaborativa **l'attività di controllo del Garante st**esso.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

	SCHEDA REGISTRO DEI TRATTAMENTI [per i contenuti vedi Faq sul registro delle attività di trattamento: https://www.garanteprivacy.it/regolamentoue/registro]							
	TITOLARE/CONTITOLARE/RAPPRESENTANTE DEL TITOLARE [inserire la denominazione e i dati di contatto]							
	RESPONSABILE DELLA PROTEZIONE DEI DATI [inserire la denominazione e i dati di contatto]							
	TIPOLOGIA DI TRATTAMENTO	FINALITA' E BASI LEGALI DEL TRATTAMENTO	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CATEGORIE DI DESTINATARI [indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI [indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

REGISTRO DEL TRATTAMENTO

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Gestione contabilità generale e IVA	Gestione contabilità generale e IVA	Ordinari – Particolari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Trasmissione delle distinte pagamenti	Trasmissione delle distinte pagamenti	Ordinari – Particolari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Trasmissioni telematiche	Trasmissione telematica: Modello 730 e 770 - Comunicazione dati fatture - Modello IVA - Modello Redditi Persone Fisiche - Società di Persone - Società di Capitali ed Enti non Commerciali - Modello Intrastat - Comunicazione beni in godimento ai soci - Comunicazione operazioni non euro - Polivalente - Altri dichiarativi fiscali n.c.	Ordinari – particolari – sanitari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Redazione documenti di bilancio (Bilancio XBRL,verbali,ecc.)	Redazione documenti di bilancio e loro allegati	Ordinari – particolari – giudiziari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Gestione Beni ammortizzabili	Gestione Ammortamento Beni	Ordinari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Presentazione Certificazione Utili e altri Proventi Corrisposti	Presentazione Certificazione Utili e altri Proventi Corrisposti	Ordinari – Particolari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Presentazione pratiche al Registro delle Imprese	Deposito Bilanci, Bollatura libri sociali	Ordinari – particolari – giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Calcolo delle imposte	Calcolo delle imposte IMU - TASI - ISCOP - IVA - IRAP	Ordinari – particolari – giudiziari	Dipendenti - Amministratori - Collaboratori - Tirocinanti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Fatturazione Attiva e Passiva	Preventivi, Contratti, Ordini, DDT, Mandati, Avvisi di parcella, Fatture	Ordinari – particolari – sanitari - giudiziari	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti – Interessati per accesso agli atti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Presentazione modelli di versamento	Presentazione modelli di versamento (F24 e F23)	Ordinari – particolari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Antiriciclaggio	Obblighi e adempimenti in materia di antiriciclaggio	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Revisione contabile / legale	Controllo e revisione contabilità - bilanci	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, Enti pubblici e privati, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Analisi di Bilancio	Valutazione performance aziendali e comparazioni fra aziende (Analisi di Bilancio, Basilea2, Benchmarking)	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI				AREA SERVIZI AMMINISTRATIVI					
Trattamento (Attività)	**Finalità**		**Categorie di dati personali**	**Categorie di interessati**		**Misure di sicurezza tecniche e organizzative**		**Categorie dei destinatari delle comunicazioni dei dati personali**	**Termini ultimi per la cancellazione delle diverse categorie di dati**
Gestione acquisti di beni e servizi e relativi contratti	acquisizione beni e servizi		Ordinari – Particolari	Imprese individuali o società che forniscono beni e servizi		Vedere scheda apposita		Ufficio amministrazione, Consulente esterno	A norma di legge
Incarichi professionali e relativi contratti	conferimento incarichi professionali		Ordinari – Particolari	Liberi professionisti o dipendenti con incarichi esterni		Vedere scheda apposita		Ufficio amministrazione, Consulenti esterni	A norma di legge
Sorveglianza sanitaria e attività di formazione obbligatoria	attività obbligatoria in base alla normativa sulla sicurezza		Ordinari – Particolari	Dipendenti - Amministratori - Collaboratori - Tirocinanti		Vedere scheda apposita		Medico Competente – Organi Pubblici di vigilanza in caso di ispezioni	A norma di legge
Conservazione archivio cartaceo atti gestionali	attività obbligatoria in base a norme di buona amministrazione		Ordinari – Particolari	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti – Interessati per accesso agli atti		Vedere scheda apposita		Nessuna trasmissione all'esterno; solo nel caso di richiesta di accesso agli atti da parte di diretti interessati aventi diritto	A norma di legge
Protocollazione posta	attività obbligatoria in base a norme di buona amministrazione		Ordinari – particolari – giudiziari	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti – Interessati per accesso agli atti		Vedere scheda apposita		In base alle richieste degli uffici	A norma di legge

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Presentazione Certificazione Utili e altri Proventi Corrisposti	Presentazione Certificazione Utili e altri Proventi Corrisposti	Ordinari – Particolari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi - Utenti - Clienti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Presentazione pratiche al Registro delle Imprese	Deposito Bilanci, Bollatura libri sociali	Ordinari – particolari – giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Calcolo delle imposte	Calcolo delle imposte IMU - TASI - ISCOP - IVA - IRAP	Ordinari – particolari – giudiziari	Dipendenti - Amministratori - Collaboratori - Tirocinanti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Fatturazione Attiva e Passiva	Preventivi, Contratti, Ordini, DDT, Mandati, Avvisi di parcella, Fatture	Ordinari – particolari – sanitari - giudiziari	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti – Interessati per accesso agli atti	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Presentazione modelli di versamento	Presentazione modelli di versamento (F24 e F23)	Ordinari – particolari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Antiriciclaggio	Obblighi e adempimenti in materia di antiriciclaggio	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Revisione contabile / legale	Controllo e revisione contabilità - bilanci	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, Enti pubblici e privati, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni
Analisi di Bilancio	Valutazione performance aziendali e comparazioni fra aziende (Analisi di Bilancio, Basilea2, Benchmarking)	ordinari – particolari - giudiziari	Ditta/Contribuente (persona fisica) Soci, collaboratori e associati, appresentante Legale Delegato/sottoscrittore Amministratori, sindaci e revisori	Vedere scheda apposita	Categorie di soggetti per cui la comunicazione è strettamente necessaria, funzionale e compatibile con la base giuridica che regolamenta il trattamento dei dati	10 anni

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Pagamento fatture dei fornitori	Istituzionali	ordinari	Amministratori - Dipendenti - Collaboratori - Fornitori di prestazioni o servizi	Vedere scheda apposita	Ufficio amministrazione, Consulente esterno, Banche	A norma di legge
Pagamento stipendi ai dipendenti	istituzionali	ordinari – particolari	Amministratori - Dipendenti - Collaboratori	Vedere scheda apposita	Ufficio amministrazione, Consulente esterno, Banche	A norma di legge
Attività di revisione o recupero crediti	Istituzionali	ordinari	Clienti	Vedere scheda apposita	Società incaricata del recupero crediti	A norma di legge
gestione Sicurezza a norma del D.Lgs. n. 81 del 2008	Istituzionali	ordinari	Dipendenti - Amministratori - Collaboratori - Tirocinanti	Vedere scheda apposita	Ufficio amministrazione, Consulente esterno	A norma di legge

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI				AREA SERVIZI PERSONALE					
Trattamento (Attività)	**Finalità**		**Categorie di dati personali**	**Categorie di interessati**		**Misure di sicurezza tecniche e organizzative**		**Categorie dei destinatari delle comunicazioni dei dati personali**	**Termini ultimi per la cancellazione delle diverse categorie di dati**
gestione denunce di infortunio (INAIL)	gestione rapporto di servizio - denunce di infortunio (INAIL)		identificativi	Dipendenti		Vedere scheda apposita		Dipendenti	cessazione dal servizio
consultazione certificati medici INPS	gestione del rapporto di servizio - consultazione certificati medici INPS		identificativi	Dipendenti		Vedere scheda apposita		Dipendenti	cessazione dal servizio
ufficio protocollo	gestione del protocollo		identificativi	Dipendenti		Vedere scheda apposita		Utenti	termini di cui al D.Lgs. 82/2009
Corsi formazione e aggiornamento del personale	Adempimento obbligo legale		Dati identificativi, personali e professionali	Dipendenti - Professionisti esterni		Vedere scheda apposita		Dipendenti - Professionisti esterni	Archivio informatico da aggiornare periodicamente. Per i cv dei dipendenti, cancellazione in caso di termine rapporto lavoro
Pratiche previdenziali	Adempimento obbligo legale		Dati identificativi, economici ed eventuali dati inerenti la salute	Dipendenti		Vedere scheda apposita		Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni	Termini di cancellazione
Assegni familiari	Adempimento obbligo legale	Dati identificativi, economici ed eventuali dati inerenti la salute.	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Stipendi	Adempimento obbligo legale	Dati identificativi, economici ed eventuali sensibili.	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Trasferte	Adempimento obbligo legale	Dati identificativi ed economici	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Assenze non contenente dati sensibili (ferie, aspettative, ecc..)	Adempimento obbligo legale	Dati identificativi	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Part-time	Adempimento obbligo legale	Dati identificativi	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Legge 104	Adempimento obbligo legale	Dati identificativi e sensibili	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Permessi per motivi personali e congedi per gravi motivi	Adempimento obbligo legale	Dati identificativi ed eventuali sensibli	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Visite fiscali	Adempimento obbligo legale	Dati identificativi e sensibili	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Elenco congedi maternità, paternità e parentali	Adempimento obbligo legale	Dati identificativi e sensibili	Dipendenti	Vedere scheda apposita	Dipendenti	Archivio informatico: cancellazione al momento del termine rapporto di lavoro. Archivio cartaceo: viene collocato nell'archivio storico
Domande assunzione e relativo c.v. allegato	Altre specifiche e diverse finalità	Dati identificativi, ed inerenti lo stile di vita	Dipendenti	Vedere scheda apposita	Dipendenti	termine di conservzione del fascicolo, salvo diverso termine stabilito dalla legge

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI			AREA SERVIZI SICUREZZA			
Trattamento (Attività)	**Finalità**	**Categorie di dati personali**	**Categorie di interessati**	**Misure di sicurezza tecniche e organizzative**	**Categorie dei destinatari delle comunicazioni dei dati personali**	**Termini ultimi per la cancellazione delle diverse categorie di dati**
sistema telecamere a circuito chiuso esterne agli uffici	Sicurezza	identificativi	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti	sistemi di autenticazione; sistemi di protezione con videosorveglianza ; registrazione accessi; porte, armadi e contenitori dotati di serrature	persone fisiche e persone giuridiche	7 giorni
sistema impianti allarme anti-intrusione	Tutela dei beni	identificativi	Dipendenti – Amministratori – Collaboratori – Tirocinanti - Liberi professionisti – Imprese o società che forniscono beni e servizi – Enti di formazione – Istituzioni varie pubbliche o private – Clienti dei servizi gestiti	sistemi di autenticazione; sistemi di protezione con videosorveglianza ; registrazione accessi; porte, armadi e contenitori dotati di serrature	persone fisiche e persone giuridiche	7 giorni

L'informativa estesa sul trattamento dati, effettuato tramite il sistema di videosorveglianza, è disponibile presso la sede dello studio professionale del Dr. XXXXYYYYYin forma cartacea, richiesta via email agli indirizzi sotto indicati oppure scaricata in formato digitale tramite il QRcode sopra riportato

LA REGISTRAZIONE È EFFETTUATA DALLA MONDIALPOL SECURITY SPA

Titolare del trattamento è il Dr. XXXXYYYYY(art. 24 Reg. UE 2016/679), quale rappresentante legale dello Studio Professionale relativamente a tutte le attività svolte per la gestione dello studio professionale, contattabile ai seguenti indirizzi:

Via VVVVVVVV,n 2 CAP - CITTA'

Email: palermo@lxxx.it Pec: dr. XXXXXYYYY@pec.it

FINALITA' DEL TRATTAMENTO, BASE GIURIDICA E TEMPI DI CONSERVAZIONE

La finalità del trattamento è la sicurezza e la tutela delle persone e del patrimonio aziendale. La liceità del trattamento trova fondamento nel perseguimento del legittimo interesse del titolare (art. 6, par. 1, lett. f) del GDPR). Le immagini riprese dalle telecamere di videosorveglianza saranno conservate per un periodo massimo di 48 ore, trascorse le quali verranno automaticamente cancellate, salvo richiesta esplicita da parte di pubbliche autorità allo scopo legittimate.

I dati personali non sono oggetto di alcun processo decisionale automatizzato (compresa la profilazione), non vengono diffusi e non saranno trasferiti al di fuori dello spazio UE.

DIRITTI DELL'INTERESSATO

In caso di domande o richieste sulla presente informativa, può inoltrarle all'indirizzo di posta elettronica: palermo@lxxx.it o all'indirizzo: Via VVVVVVVV,n 2 CAP - CITTA', per esercitare i diritti di accesso, modifica, integrazione e cancellazione, previsti dall'art. 15 del reg. Ue 679/2016 (GDPR). Per tutti i dettagli, consultare le informazioni fornite dal titolare del trattamento attraverso l'informativa estesa (reperibile nelle modalità sopra indicate).

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI — AREA SERVIZI INFORMATICI

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Dematerializzazione documenti	Gestione Archivi	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	software	Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	10 anni
Distruzione documenti	Gestione Archivi	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Distruggidocumenti	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
Assistenza IT/HW	Gestione, da remoto e on site, delle infrastrutture IT	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	manutenzione on-site e da remoto	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
Assistenza SW	Assistenza software da remoto e on-site	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	manutenzione on-site e da remoto	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Archivi digitali e Data Base	Gestione Archivi digitali	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	server, nas, server di backup	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	10 anni
Assistenza server e nas	Gestione infrastrutture IT	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	server, nas, server di backup	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
Back up dati	Protezione dati	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Server locali - Server di backup in remoto	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A

Trattamento (Attività)	Finalità	Categorie di dati personali	Categorie di interessati	Misure di sicurezza tecniche e organizzative	Categorie dei destinatari delle comunicazioni dei dati personali	Termini ultimi per la cancellazione delle diverse categorie di dati
Area Web Riservata	Trasmissione dati	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Piattaforma web - server	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
Sito Web	Comunicazioni ed informazioni alla clientela	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Web server	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
Rete Intranet	Gestione attività operative	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Switch ed apparati di rete	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	N/A
posta elettronica	Comunicazioni	Dati di identificazione, contatto, finanziari, economici, fiscali, contabili, Giudiziari, Qualifiche ed esperienze professionali.	Clienti, Fornitori, Dipendenti, Collaboratori, Soci	Mail server	Soci, Clienti, Fornitori, Dipendenti, Collaboratori, Enti Pubblici, interessato	10 anni

rischi		descrizione dell'impatto sulla sicurezza	Gravità e probabilità alta/media/bassa
comportamenti degli operatori	sottrazione di credenziali di autenticazione	accesso non autorizzato al computer	Gravità alta/probabilità bassa
	carenza di consapevolezza, disattenzione, incuria	le credenziali perdono riservatezza o dati sono inutilmente resi visibili	Gravità alta/probabilità bassa
	comportamenti sleali o fraudolenti	accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da incaricati che non ne hanno diritto	Gravità alta/probabilità bassa
	errore materiale	cancellazione o perdita di dati	Gravità alta/probabilità bassa esiste copia cartacea di parte dei documenti; è attivo un sistema di backup giornaliero gli operatori sono adeguatamente formati all'utilizzo delle procedure.

REGISTRO DEL TRATTAMENTO

rischi		descrizione dell'impatto sulla sicurezza	Gravità e probabilità alta/media/bassa
eventi relativi agli strumenti	azione di virus informatici o di programmi suscettibili di recare danno	cancellazione di dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	Gravità alta/probabilità bassa - è installato un sistema antivirus di ultima generazione
	spamming o tecniche di sabotaggio	confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore	Gravità media/probabilità bassa - è installato un sistema antispamming
	malfunzionamento, indisponibilità o degrado degli strumenti	malfunzionamenti o blocco del sistema con impossibilità al trattamento	Gravità media/probabilità bassa - è in atto una costante manutenzione degli strumenti
	accessi esterni non autorizzati	visione indebita di dati o sabotaggio	Gravità alta/probabilità bassa - rete protetta da firewall
	intercettazione di informazioni in rete	visione indebita di dati	Gravità alta/probabilità bassa - rete protetta da firewall

REGISTRO DEL TRATTAMENTO

rischi		descrizione dell'impatto sulla sicurezza	Gravità e probabilità alta/media/bassa
eventi relativi al contesto	ingressi non autorizzati a locali/aree ad accesso ristretto	sabotaggio delle macchine, con eventuale perdita di dati; accesso abusivo se le credenziali fossero lasciate disponibili	sabotaggio:gravità media/probabilità bassa altro: gravità alta/probabilità bassa: gli operatori sono adeguatamente istruiti
	sottrazione di strumenti contenenti dati	perdita di dati, rallentamento o blocco dell'attività per carenza di computer	Gravità bassa/ probabilità media - dati non visibili in quanto residenti sul server per le macchine collegate alla rete.
	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, …), nonché dolosi, accidentali o dovuti a incuria	perdita di dati, rallentamento o blocco dell'attività per carenza di computer	Gravità media/ probabilità bassa
	guasto a sistemi complementari (impianto elettrico, climatizzazione, etc…)	perdita di dati e blocco del sistema con riferimento alla macchina server; surriscaldamento dei computers e in particolare della scheda madre o altre componenti, con possibilità di guasto	Gravità media/probabilità bassa - adeguamento del sistema elettrico della sede centrale ove ubicato il server
	errori umani nella gestione della sicurezza fisica	danni agli strumenti, con possibile perdita di dati e malfunzionamenti	Gravità media/probabilità bassa

REGISTRO DEL TRATTAMENTO

MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE PER DATI TRATTATI CON STRUMENTI ELETTRONICI					
misure	descrizione dei rischi	trattamenti interessati	misure in essere	misure da adottare e tempi previsti per l'adozione	struttura addetta all'adozione
istruzioni agli incaricati		Tutti i trattamenti informatizzati	Sì	(ad ogni nuova assunzione o incarico)	Tutte le Aree
formazione		Tutti i trattamenti informatizzati	Sì	(ad ogni nuova assunzione o incarico o variazione di mansione)	Area Amministrativa
azione del "custode delle parole-chiave" presenza di: antivirus antispamming firewall	Eventi relativi ai comportamenti degli operatori:			pianificazione di una procedura di modifica periodica delle credenziali di autenticazione (p.w. scade automaticamente ogni 6 mesi per i dati ordinari e ogni 3 mesi per i dati sensibili) - pianificazione di una procedura che preveda l'utilizzo delle credenziali di un incaricato assente	Area Amministrativa – Responsabile custodia password
	furto delle credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria;	Tutti i trattamenti informatizzati	Sì		
	comportamenti sleali o fraudolenti;				
	azione di virus informatici o di codici malefici spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio intercettazione di informazioni in rete				
controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Tutti i trattamenti informatizzati	Sì	adozione di un screensaver protetto da password;	Tutte le Aree
creazione di profili di autorizzazione diversificati					
	errore materiale	Tutti i trattamenti informatizzati	Sì	/	Tutte le Aree

CO•NE•PRO
COMMERCIALISTI NETWORK PROFESSIONALE

REGISTRO DEL TRATTAMENTO

misure	descrizione dei rischi	trattamenti interessati	misure in essere	misure da adottare e tempi previsti per l'adozione	struttura addetta all'adozione
presenza di: antivirus antispamming firewall	eventi relativi agli strumenti: - azione di virus informatici o di codici malefici; - spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio; - malfunzionamento, indisponibilità o degrado degli strumenti; - accessi esterni telematici non autorizzati; - intercettazione di informazioni in rete	Tutti i trattamenti informatizzati	Sì	/	Tutte le Aree
istruzioni agli incaricati atte a individuare e prevenire le situazioni a rischio		Tutti i trattamenti informatizzati	Sì	(*) (ad ogni nuova assunzione o incarico)	Tutte le Aree
formazione degli incaricati a riconoscere i messaggi di disturbo		Tutti i trattamenti informatizzati	Sì	(*) (ad ogni nuova assunzione o incarico)	Tutte le Aree
piano di backup - disaster recovery e di continuità operativa		Tutti i trattamenti informatizzati	Sì Relativamente al sistema di backup	/	Tutte le Aree
installazione di firewall, con regolare aggiornamento		Tutti i trattamenti informatizzati	Sì Presenza di apposito firewall	/	Tutte le Aree
eventuale adozione di cifratura per proteggere i dati più gravi		Tutti i trattamenti informatizzati	/	- eventuale adozione delle possibili misure volte ad evitare la visualizzazione in chiaro dei dati più gravi in associazione alle generalità dell'interessato.	Aree interessate a seconda dei casi

REGISTRO DEL TRATTAMENTO

misure	descrizione dei rischi	trattamenti interessati	misure in essere	misure da adottare e tempi previsti per l'adozione	struttura addetta all'adozione
chiusura a chiave dei locali quando non presidiati	eventi relativi al contesto: accessi non autorizzati ai locali; asportazione e furto di strumenti contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc...); errori umani nella gestione della sicurezza fisica	Tutti i trattamenti informatizzati	Sì	(*) (ad ogni nuova assunzione o incarico)	Tutte le Aree
disponibilità di estintori come da normativa anti-incendio		Tutti i trattamenti informatizzati	Sì	/	RSPP
Il backup avviene in due diversi dispositivi NAS che si trovano 1 nella sede centrale e l'altro in edificio separato in stanza chiusa a chiave		Tutti i trattamenti informatizzati	Sì	/	CED
verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		Tutti i trattamenti informatizzati	Sì	/	Responsabile Gestione patrimonio
verifica della logistica degli apparecchi e del loro corretto posizionamento		Tutti i trattamenti informatizzati	Sì	/	Tutte le Aree
gruppo di continuità		Tutti i trattamenti informatizzati	Sì	/	CED

REGISTRO DEL TRATTAMENTO

MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE PER DATI TRATTATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI					
misure	descrizione dei rischi	trattamenti interessati	misure in essere	misure da adottare e tempi previsti per l'adozione	struttura addetta all'adozione
istruzioni agli incaricati	Eventi relativi ai comportamenti degli operatori: carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; accessi esterni non autorizzati errore materiale	Tutti i trattamenti cartacei	Sì	/	Tutte le Aree
custodia dei documenti in armadi chiusi a chiave		Tutti i trattamenti cartacei	Sì, in tutti gli armadi in dotazione	verifica periodica del buon funzionamento delle serrature degli armadi	Tutte le Aree
controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Tutti i trattamenti cartacei	Sì	/	Tutte le Aree
chiusura a chiave dei locali quando non presidiati: istruzioni a tutti gli operatori	eventi relativi al contesto: accessi non autorizzati ai locali; asportazione e furto di fascicoli (o altri contenitori) contenenti dati; eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria;guasto ai sistemi comple- mentari (impianto elettrico, climatizzazione, etc...); errori umani nella gestione della sicurezza fisica	Tutti i trattamenti cartacei	Sì	/	Tutte le Aree
disponibilità di estintori come da normativa anti-incendio		Tutti i trattamenti cartacei	Sì	/	Tutte le Aree – Responsabile Servizio di Prevenzione e Protezione
				verifica periodica del buon funzionamento delle serrature degli armadi	
Disponibilità di armadi muniti di chiusura a chiave		Tutti i trattamenti cartacei	Sì		Tutte le Aree
verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		Tutti i trattamenti cartacei	Sì	/	Responsabile Servizio di Prevenzione e Protezione

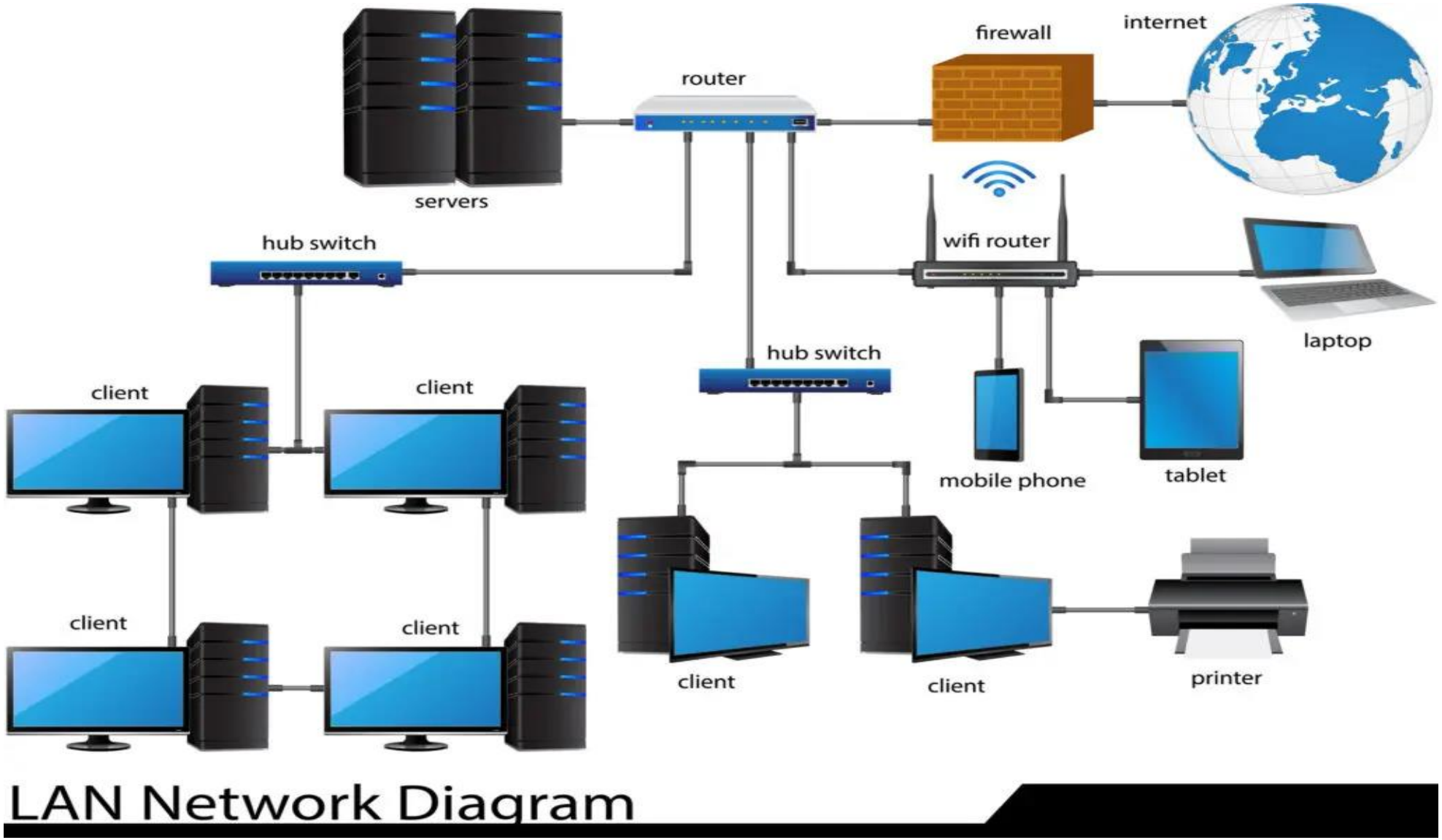
REGISTRO DEL TRATTAMENTO

CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI			
Banca dati/data base /archivio di dati	criteri e procedure per il salvataggio dei dati (backup)	criteri e procedure per il ripristino dei dati	Pianificazione delle prove di ripristino
Tutta la gestione documentale, tutte le banche dati /archivi e documenti presenti/elaborati/conservati in tutte le Aree della Struttura - e tutte le strutture applicative e software applicativi memorizzati in server virtuali	la gestione documentale è memorizzata all'interno di un dispositivo NAS, il backup viene effettuato giornalmente in automatico dal programma di Backup installato e viene salvato in un NAS ulteriore che si trova in un edificio separato da quello in cui è situato il primo NAS al fine di garantire la sicurezza di conservazione di almeno 1 NAS nel caso di gravi incidenti alla struttura (incendi, crolli ecc..) - il backup dei server virtuali viene effettuato anch'esso giornalmente in automatico dal programma di Backup installato e controllato dalla società incaricata. - tutte le attività di backup vengono svolte con tempi di ritenzione di 30 gg. (retention time).	Il ripristino delle singole banche dati è possibile mediante l'apposita procedura di backup che gestisce anche il ripristino.	La prova di ripristino è stata effettuata all'atto dell'adozione della procedura di copia. La sua efficacia viene verificata semestralmente dalla società incaricata

REGISTRO DEL TRATTAMENTO

ATTIVITA' AFFIDATE ALL'ESTERNO CHE COMPORTANO TRATTAMENTO DI DATI PERSONALI		
descrizione sintetica dell'attività esternalizzata	soggetto esterno	descrizione dei criteri e degli impegni assunti per l'adozione delle misure
Gestione economica del personale e consulenza in materia di gestione giuridica/organizzativa e consulenza in materia contrattualistica dello Studio	Consulente del lavoro, consulente fiscale, consulente legale	Il professionista incaricato si impegna a trattare i dati personali degli interessati ai soli fini dell'espletamento dell'incarico ricevuto, adempiendo agli obblighi previsti dal Codice per la protezione dei dati personali. Si impegna inoltre, a relazionare annualmente sulle misure di sicurezza adottate e ad informare il titolare del trattamento in caso di situazioni anomale o di emergenze. I contraenti si impegnano a condividere gli interventi volti al corretto trattamento dei dati personali, integrando eventualmente le procedure in essere laddove ne venga rilevata la necessità o l'opportunità.
Consulenza in materia assicurativa – Brokeraggio assicurativo - Servizio di copertura Polizze Assicurative	Consulente assicurativo	Contratto sottoscritto con impegno da parte dello Studio a: trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto; ad adempiere agli obblighi previsti dal Codice per la protezione dei dati; al rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali anche integrando procedure già in essere; a relazionare periodicamente sulle misure di sicurezza adottate e ad informare il titolare del trattamento in caso di situazioni anomale o di emergenze
Manutenzione hardware e software sul Server e sul Nas e sugli apparati router e firewall; monitoraggio sistema antivirus e verifica aggiornamenti;	Consulente HW e SW	Contratto sottoscritto con impegno da parte dello Studio a: trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto; ad adempiere agli obblighi previsti dal Codice per la protezione dei dati; al rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali anche integrando procedure già in essere; a relazionare periodicamente sulle misure di sicurezza adottate e ad informare il titolare del trattamento in caso di situazioni anomale o di emergenze
Servizi ex DLgs 81/2008 – funzioni di RSPP	Consulente RSPP	Contratto sottoscritto con impegno da parte della Ditta a: trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto; ad adempiere agli obblighi previsti dal Codice per la protezione dei dati; al rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali anche integrando procedure già in essere; a relazionare periodicamente sulle misure di sicurezza adottate e ad informare il titolare del trattamento in caso di situazioni anomale o di emergenze
Contratto per erogazione del servizio di conservazione digitale di documenti informatici	Fornitore PEC	Contratto sottoscritto con impegno da parte dello Studio a: trattare i dati ai soli fini dell'espletamento dell'incarico ricevuto; ad adempiere agli obblighi previsti dal Codice per la protezione dei dati; al rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali anche integrando procedure già in essere; a relazionare periodicamente sulle misure di sicurezza adottate e ad informare il titolare del trattamento in caso di situazioni anomale o di emergenze

REGISTRO DEL TRATTAMENTO IT



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Attacchi informatici, il ministro dell'interno Piantedosi: 'Aumentati del 115% nell'ultimo anno. L’Italia eccelle nella protezione delle infrastrutture critiche'

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CryptoLocker
Payment for private key
bitcoin
• Choose the amount of payment:
2 BTC
• Send coins to the following address:
Attention!
Make sure that you enter the payment information correctly! Each incorrect attempt will reduce the time to destroy the private key in half!
Are you sure you entered your payment information correctly?
Yes
No
Time left
43 : 30 : 40
<< Back
PAY

Notifica di consegna mancata DHL

Oggetto: Notifica di consegna mancata DHL
Mittente: DHL Express <martinarossi.dhl@gmail.com>
Data: 13/12/2018, 09:58
A: undisclosed-recipients:;

Caro cliente,

Abbiamo tentato di consegnare il tuo articolo alle 8:10 del 12 dicembre 2008. (Leggi i dettagli del file allegato)

Il tentativo di consegna non è riuscito perché nessuno era presente all'indirizzo di spedizione, quindi questa notifica è stata inviata automaticamente

Se il pacco non è programmato per la riconsegna o ritirato entro 72 ore, verrà restituito al mittente.

Numero di etichetta: DHL737215637AA

Data di consegna prevista: 12,2018 dicembre

Classe: Servizi del pacchetto

Servizio: conferma di consegna

Stato: eNotification inviata

Leggi il file allegato per i dettagli.

DHL Customer Service.
2018 © DHL International. All rights reserved.

Allegati:

Delivery Note - AWD 72703432141- 0092203960288.pdf.gz 348 kB

Notifica di consegna mancata DHL

Oggetto: Notifica di consegna mancata DHL
Mittente: DHL Express <martinarossi.dhl@gmail.com>
Data: 12/12/2018, 09:58
A: undisclosed-recipients:;

Caro cliente,

Abbiamo tentato di consegnare il tuo articolo alle 8:10 del 12 dicembre 2008. (Leggi i dettagli del file allegato)

Il tentativo di consegna non è riuscito perché nessuno era presente all'indirizzo di spedizione, quindi questa notifica è stata inviata automaticamente

Se il pacco non è programmato per la riconsegna o ritirato entro 72 ore, verrà restituito al mittente.

Numero di etichetta: DHL737215637AA

Data di consegna prevista: 12,2018 dicembre

Classe: Servizi del pacchetto

Servizio: conferma di consegna

Stato: eNotification inviata

Leggi il file allegato per i dettagli.

DHL Customer Service.
2018 © DHL International. All rights reserved.

Allegati:

Delivery Note - AWD 72703432141- 0092203960288.pdf.gz 348 kB

Oggetto: Avviso di rimborso!
Mittente: "Agenzia delle Entrate" <info@agenziadelleentrat.it>
Data: 17/02/2021, 03:58
A: "rpd@clinicacandela.it" <rpd@clinicacandela.it>

Gentile cliente,

Hai diritto a un rimborso fiscale di € 136,99.
Invia il modulo sottostante in modo che possiamo elaborarlo
rimborso il prima possibile.

Accesso al rimborso

Dopo aver ricevuto il modulo, verrà addebitato il rimborso
considerazione per i nostri Servizi.
L'invio di un file non valido o la registrazione dopo un certo limite può
ritardare il rimborso
Riceverai presto un modulo di rimborso

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Oggetto: Avviso di rimborso!
Mittente: "Agenzia delle Entrate" <info@agenziadelleentrat.it>
Data: 17/02/2021, 03:58
A: "rpd@clinicacandela.it" <rpd@clinicacandela.it>

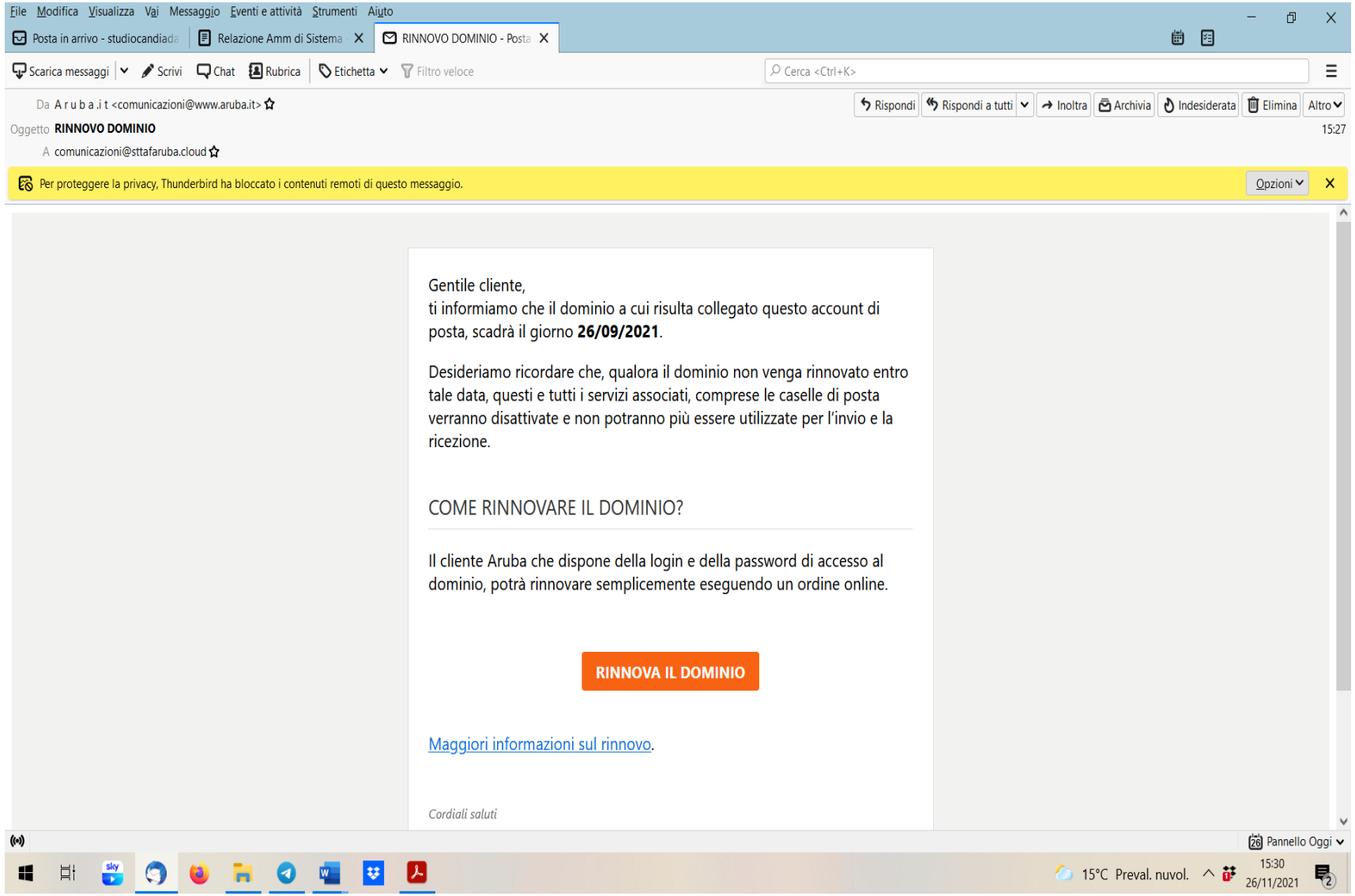
Gentile cliente,

Hai diritto a un rimborso fiscale di € 136,99.
I[illegible]nte in modo che possiamo elaborarlo
[illegible]mborso il prima possibile.

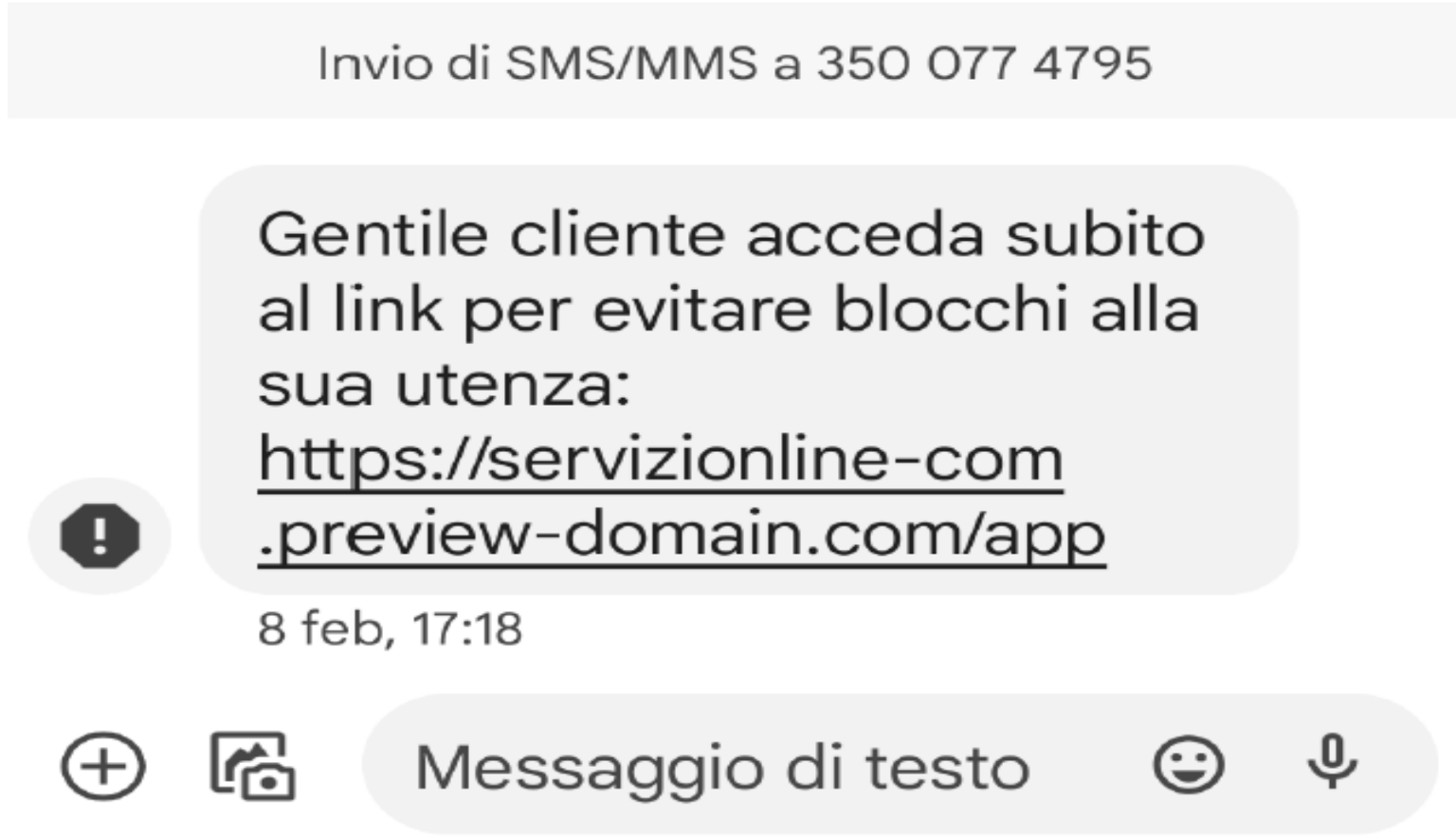
Accesso al rimborso

Dopo aver ricevuto il modulo [illegible]errà addebitato il rimborso
[illegible]onsiderazione per i nostri S[illegible]vizi.
[illegible]avio di un file non valido[illegible] la registrazione dopo un certo limite può
rita[illegible] il rimborso.
Riceverai presto un modulo di rimborso

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

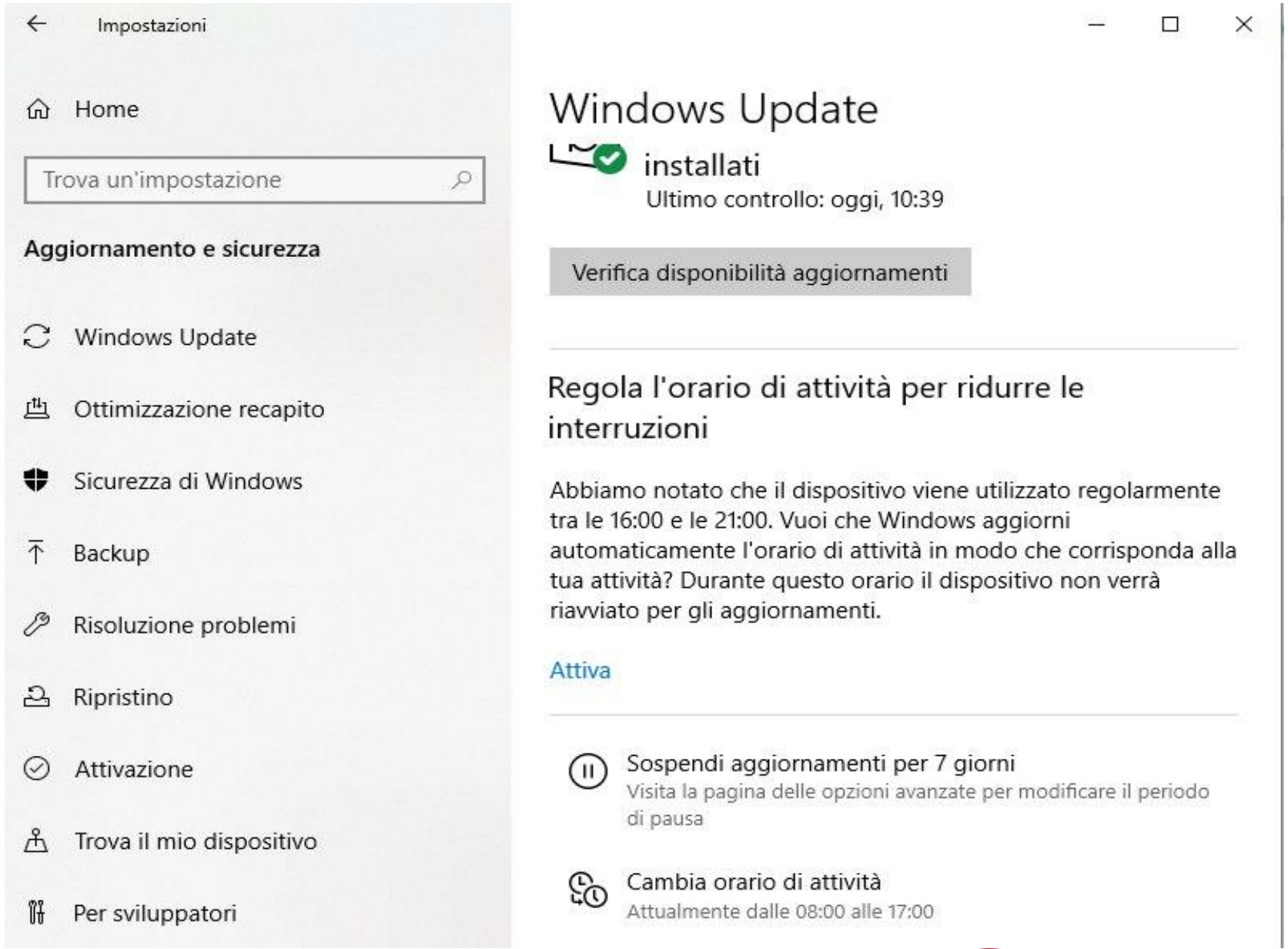


CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

UniCredit

Milano, 28.10.2019

0053
P7P90309458000100001 01 9M01
31406640 MTAS5114801164S
3320 2
99999

[redacted]

PLF61JAVASY03894C05D

Gentile Signora/Signore,

ci preme comunicarLe che abbiamo individuato un accesso non autorizzato ad alcuni dati, tra cui i Suoi.

I dati in questione, che risalgono al 2015, sono esclusivamente di carattere anagrafico ed in particolare riguardano **nome e cognome, comune e provincia di riferimento, numero di telefono cellulare, indirizzo email**.

Alla luce del fenomeno, comune a tutto il sistema, di sempre più numerosi tentativi di utilizzo non lecito dei canali digitali – come ad esempio tentativi di phishing o altri contatti non autorizzati che potrebbero risultare dall'utilizzo di informazioni anagrafiche quali quelle in oggetto - speriamo di fare cosa utile fornendo **in allegato una serie di regole di comportamento** per rendere la navigazione su internet e l'utilizzo dei canali digitali sempre più sicuri.

UniCredit è fortemente impegnata nel garantire la protezione dei dati della propria clientela ed ha implementato processi che hanno significativamente rafforzato la capacità di garantire sicurezza e protezione ai propri clienti. In particolare dallo scorso luglio 2019, l'accesso ai canali *web* e *mobile* avviene in modo ancora più sicuro grazie alla **SCA - Strong Customer Authentication** - e la conferma degli ordini di pagamento avviene attraverso l'uso di un codice autorizzativo che integra sia l'importo sia il beneficiario del pagamento. Oltre al **Mobile Token** e alle **chiavette generatrici di codici usa e getta**, rese opportunamente conformi alla normativa PSD2, è stata messa a disposizione dei clienti che hanno attivato **l'App sul proprio Smartphone**, una nuova **modalità di conferma sicura basata sulle notifiche push.**

Le confermiamo che abbiamo immediatamente adottato tutte le azioni necessarie per gestire l'accaduto ed abbiamo altresì informato tutte le autorità, compresa la polizia.

Per qualsiasi dubbio, richiesta di chiarimenti o in caso osservaste comportamenti anomali o non usuali nelle comunicazioni provenienti da UniCredit, è possibile rivolgersi al personale della **propria Filiale** o contattare il **numero verde dedicato 800.323.285** disponibile con orario esteso: **lun-ven 8-22 e sabato 9-14**. Abbiamo deciso inoltre di attivare la casella email *assistenzainternet-FPMI@unicredit.eu* cui può rivolgersi per qualsiasi chiarimento.

Cordiali saluti.

Andrea Casini   Remo Taricani
Co-CEO Commercial Banking Italy
UniCredit S.p.A.

SAMSUNG 4K ULTRA HD

4K ULTRA HD Samsung SMART TV WiFi TV DOLBY DIGITAL • PLUS

NE • PRO
TI NETWORK PROFESSIONALE

www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

SAMSUNG

BebèCare

Una soluzione innovativa che supporta le famiglie

chicco

CO • NE • PRO

COMMERCIALISTI NETWORK PROFESSIONALE

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

iOS

ANDROID

CO • NE • PRO

COMMERCIALISTI NETWORK PROFESSIONALE

EXODUS

Malware/Trojan per attività di investigazione della Procura - Polizia di Stato

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

CONTROLLO DEGLI ACCESSI	
C'è una portineria / reception sempre presidiata per l'accesso all'edificio oppure agli uffici?	
L'azienda è dotata di sistema di videosorveglianza?	
È utilizzato un registro dei visitatori?	
L'edificio / gli uffici sono protetti da un sistema di rilevamento delle intrusioni?	
Sono presenti password personali / nome utente / protezione dell'accesso ai sistemi con cui sono trattati i dati personali di cui il committente è titolare?	
Come sono concesse le autorizzazioni per l'accesso?	
Per l'amministrazione dei sistemi esiste un account ADMIN indipendente che differisce dall'account utente individuale ed effettivo dell'amministratore di sistema?	
Esistono dei parametri vincolanti per le password in azienda? In caso affermativo descriverne i requisiti.	

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

CONTROLLO DEGLI ACCESSI	
Esistono dei parametri vincolanti per le password in azienda? In caso affermativo descriverne i requisiti.	
Il sistema IT obbliga l'utente al rispetto dei predetti parametri sulla password?	
Le persone autorizzate al trattamento utilizzano account condivisi per accedere ai dati personali?	
I profili di accesso ai sistemi IT vengono riesaminati almeno una volta all'anno per verificare che siano corretti, secondo un principio di profilazione degli accessi che tenga conto del ruolo e delle responsabilità di ciascun utente/autorizzato al trattamento?	
Le credenziali di accesso sono disattivate quando l'autorizzato al trattamento non ha più diritto di accedere ai dati personali (ad esempio, per cessazione del rapporto di lavoro o cambio di mansione)?	
È stato impostato un blocco automatico dello schermo protetto da password?	

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

CONTROLLO DEGLI ACCESSI	
Descrivere le misure adottate nel caso in cui la password sia stata perduta / dimenticata / violata.	
Esistono sistemi di produzione e di test separati in caso di necessità di interventi di manutenzione ai sistemi?	
In che modo i supporti dati non più necessari (chiavette USB, dischi fissi, CD-Rom, DVD / dischetti), su cui sono memorizzati i dati personali vengono smaltiti dall'azienda?	
Come viene smaltita la documentazione non più necessaria contenente dati personali?	
I dati personali sono memorizzati fisicamente su server gestiti dal titolare o da terzi?	
La sala in cui è ubicato il server è protetta da sistema di rilevamento delle intrusioni e/o da un sistema di chiusura?	
Descrivere le modalità di gestione di un eventuale accesso da remoto (VPN / IPSec):	
C'è un limite al numero di tentativi di accesso da remoto non riusciti?	
L'accesso da remoto viene disconnesso automaticamente dopo un certo tempo di inattività?	
I sistemi con cui vengono trattati i dati personali di cui il committente è titolare sono protetti da firewall?	
In caso di trasferimento di dati, la trasmissione è criptata / protetta tecnicamente?	
Altro	

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

Integrità e disponibilità	
È necessario garantire che i dati personali siano protetti da modifica, distruzione o perdita accidentale, oltre che da accessi non autorizzati.	
I sistemi IT sono tecnicamente protetti dalla perdita dei dati / accesso ai dati non autorizzato?	
Esiste un piano di emergenza documentato (ad es. misure di emergenza in caso di difetti dell'hardware / incendio / perdita totale ecc.)?	
È stata implementata una procedura di business continuity da seguire in caso di violazione dei dati personali?	
Esiste un piano di backup documentato?	
Con quale frequenza sono realizzati i backup dei sistemi?	
Su quali strumenti è salvato il backup?	
Dove vengono conservati i backup?	
I dati di backup / i backup sono criptati?	

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

Integrità e disponibilità	
I dati di backup / i backup sono criptati?	
I dati personali sono trattati in modo pseudoanonimizzato?	
In caso come avviene la pseudoanonimizzazione?	
I dati sono trattati in modo criptato?	
In caso di trattamento in modo criptato, come avviene la cifratura?	
I soggetti (interni o esterni) che si occupano di cybersecurity sono ben identificati?	
Esistono linee guida e standard per la verifica regolare della sicurezza del trattamento dei dati?	
I controlli / verifiche della sicurezza si svolgono con regolarità?	
I sistemi IT, mediante i quali vengono trattati i dati personali, sono sottoposti, almeno una volta all'anno, a penetration test o vulnerability assessment?	
Sono stati individuati i soggetti a cui comunicare i dati personali indicati nell'informativa art. 13 e 14 del GDPR?	
È stato verificato che non vi è alcun trasferimento di dati fuori dalla UE?	

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

Cancellazione e diritto di accesso	
Alla scadenza dei termini di conservazione o cancellazione i dati personali devono essere cancellati conformemente alla normativa sulla protezione dei dati personali, ossia devono essere resi completamente irriconoscibili oppure anonimi, ad es. mediante rimozione dei riferimenti personali; devono inoltre essere garantiti i diritti di cui si parla nelle informative.	
I termini di cancellazione sono documentati per ogni categoria di dati?	
Come avviene la cancellazione dei dati personali?	
I dati di un interessato possono essere cancellati su richiesta?	
Su richiesta dell'interessato, può essere fornita una copia dei dati personali memorizzati che lo riguardano?	
Ci sono di misure tecniche in grado di consentire anche la rettifica, l'aggiornamento e la limitazione del trattamento dei dati personali su richiesta del soggetto interessato?	
L'azienda dispone di misure tecniche in grado di consentire la restituzione dei dati personali su richiesta e/o al termine di un contratto come titolare / responsabile?	
Altro	

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

Misure organizzative di carattere generale	
L'organizzazione è tenuta a nominare un responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento?	
Risulta nominato per iscritto un responsabile della protezione dei dati ai sensi dell'articolo 37 del Regolamento?	
Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti mediante lettera di incarico?	
I dipendenti che trattano i dati personali ricevono una formazione documentata in materia di protezione dei dati personali?	
I dipendenti si impegnano alla riservatezza dei dati per iscritto?	
L'azienda ha nominato dei responsabili (esterni)?	
Come viene garantito che i responsabili implementino le disposizioni contrattuali e le relative direttive e misure di sicurezza?	

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CHECK LIST PER CONSULENZA PRIVACY/AUDIT DPO

Misure organizzative di carattere generale	
Sono state adottate misure organizzative interne volte a prevenire / gestire eventuali violazioni in merito al trattamento di dati personali da parte degli autorizzati al trattamento dei dati personali (procedura di data breach)?	
Esiste un indirizzo e-mail dedicato dove possono essere segnalate violazioni dei dati personali (procedura di data breach) e in generale esiste un regolamento aziendale di data breach?	
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale?	
Esiste ed è mantenuto aggiornato in inventario dei data base e archivi cartacei presenti in azienda?	
Esiste un Regolamento per l'utilizzo delle attrezzature informatiche?	
Esiste una procedura interna per dare seguito all'esercizio dei diritti dell'interessato?	

Accountability e approccio basato sul rischio

Il GDPR non ha solo ampliato i diritti riconosciuti all'interessato, ma si è concentrato sulla maggiore responsabilizzazione dei soggetti coinvolti nel trattamento dei dati personali, mostrando grande interesse al tema della data security.

Il GDPR adotta taluni "strumenti" al fine di rafforzare la tutela dei dati e la responsabilizzazione del Titolare e del Responsabile del trattamento:

- sancisce il principio di *accountability* (Art. 5, par. 2);
- sancisce i principi della *privacy by design* e della *privacy by default*;
- Prevede la tenuta del Registro dei trattamenti;
- richiede d'implementare adeguate misure di sicurezza, tenendo in considerazione le tipologie di operazioni svolte e i relativi livelli di rischio, affinché non si verifichino violazioni dei dati;
- introduce la figura del Data Protection Officer.

Il principio di *accountability* ambisce a realizzare il passaggio da una concezione di adempimento formale della normativa privacy, ad un approccio sostanziale di protezione dei dati, connesso alla natura delle attività concretamente svolte, all'analisi dei rischi e alle misure di sicurezza che risultino adeguate alle singole fattispecie.

Accountability e approccio basato sul rischio: registro dei trattamenti

GDPR: art. 30, par. 5
WP29 " Documento di sintesi sulle deroghe all'obbligo di conservazione dei registri delle attività di trattamento ai sensi dell'articolo 30(5) GDPR" – 19 aprile 2018

Nonostante sia vivamente consigliato per il titolare del trattamento tenere un proprio Registro dei trattamenti, vi sono dei casi in cui simile tenuta non è prevista come obbligatoria.

NON è obbligatoria la tenuta del Registro dei trattamenti

per

le imprese o le organizzazioni con meno di 250 dipendenti che trattano dati personali, **a meno che**

- il trattamento svolto possa presentare un rischio, anche non elevato, per i diritti e le libertà dell'interessato
- il trattamento non sia occasionale
- il trattamento coinvolga categorie particolari di dati ex art. 9 oppure dati relativi a condanne penali e a reati ex art. 10

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Accountability e approccio basato sul rischio: violazioni dei dati personali (data breach)

GDPR: artt. 4 – 33 – 34 e considerando da 85 a 88

Violazione dei dati personali (c.d. data breach) definita dall'art. 4 par. 12 GDPR come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati».

Si tentare di prevenire un data breach ponendo in essere le adeguate misure di sicurezza di cui all'art. 32 GDPR.

Il titolare deve documentare qualsiasi data breach avvenuto, le circostanze e le conseguenze ad esso relativo, e i provvedimenti adottati per porvi rimedio.

A seconda dei casi, qualora si verifichi un data breach, bisogna darne comunicazione a:

- Autorità di controllo (Art. 33 GDPR)
- Interessati coinvolti (Art. 34 GDPR)

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Accountability e approccio basato sul rischio: violazioni dei dati personali (data breach)

GDPR: artt. 4 – 33 – 34 e considerando da 85 a 88

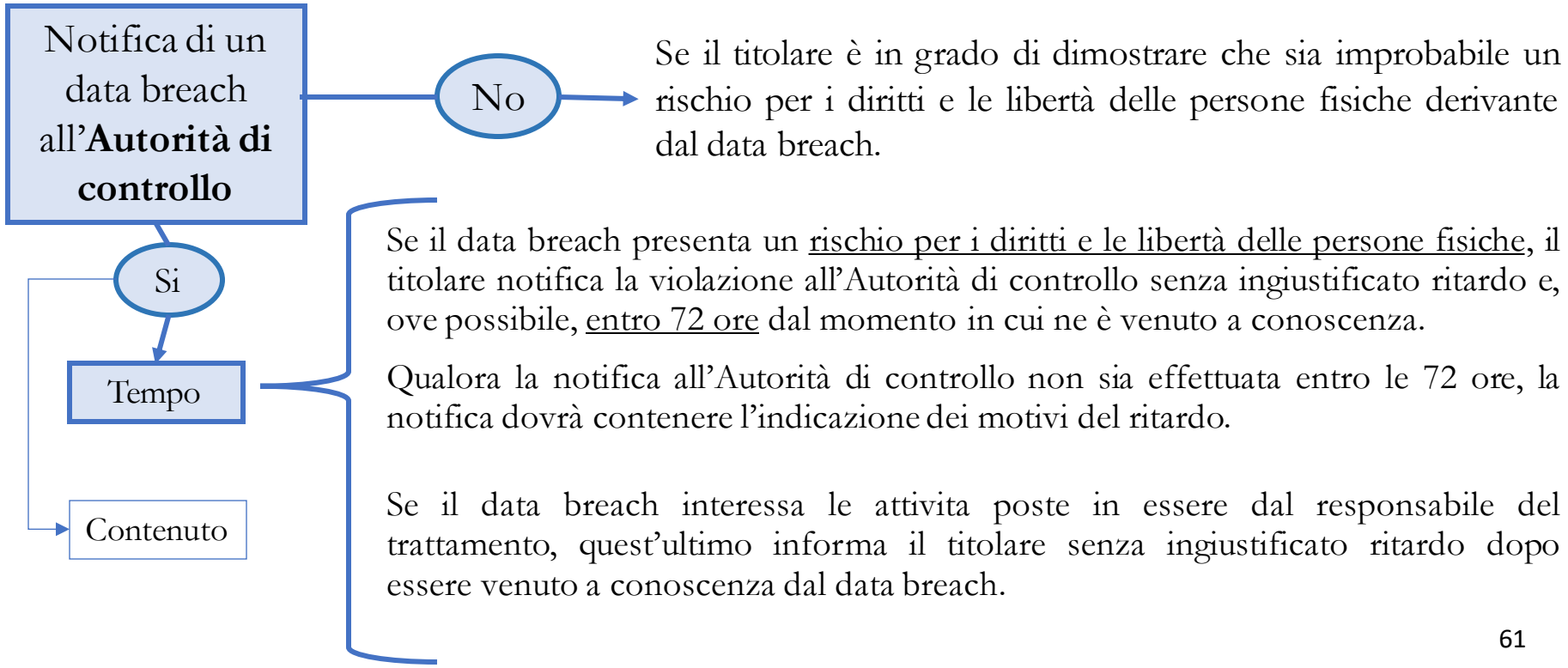
Il GDPR ha evidenziato che un data breach, se non affrontato in modo adeguato e tempestivo, può provocare **danni fisici, materiali o immateriali alle persone fisiche**.
Tra le tipologie di dati:

- perdita di controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati protetti da segreto professionale;
- in generale, qualsiasi danno economico o sociale significativo per la persona fisica.

Accountability e approccio basato sul rischio: violazioni dei dati personali (data breach)

GDPR: art. 33 e considerando 85, 87 e 88

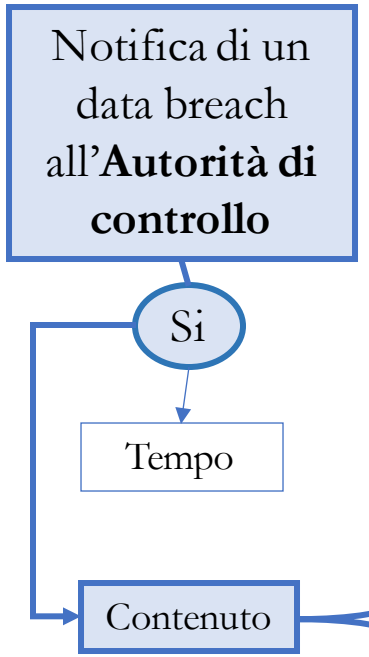
WP29 "Guidelines on Personal data breach notification under Regulation 2016/679" - Adottate 3 ottobre 2017, riviste 6 febbraio 2018



Accountability e approccio basato sul rischio: violazioni dei dati personali (data breach)

GDPR: art. 33 e considerando 85, 87 e 88

WP29 "Guidelines on Personal data breach notification under Regulation 2016/679" - Adottate 3 ottobre 2017, riviste 6 febbraio 2018



Il GDPR richiede che la notifica all'Autorità di controllo contenga:

- descrivere la natura del data breach, comprese le categorie e il numero di interessati coinvolti, nonché le categorie e il numero di registrazioni dei dati personali in questione;
- i dati di contatto del soggetto a cui rivolgersi per maggiori informazioni;
- le probabili conseguenze derivanti dal data breach;
- le misure adottate o in corso di adozione per rimediare al data breach e per attenuarne le conseguenze negative.

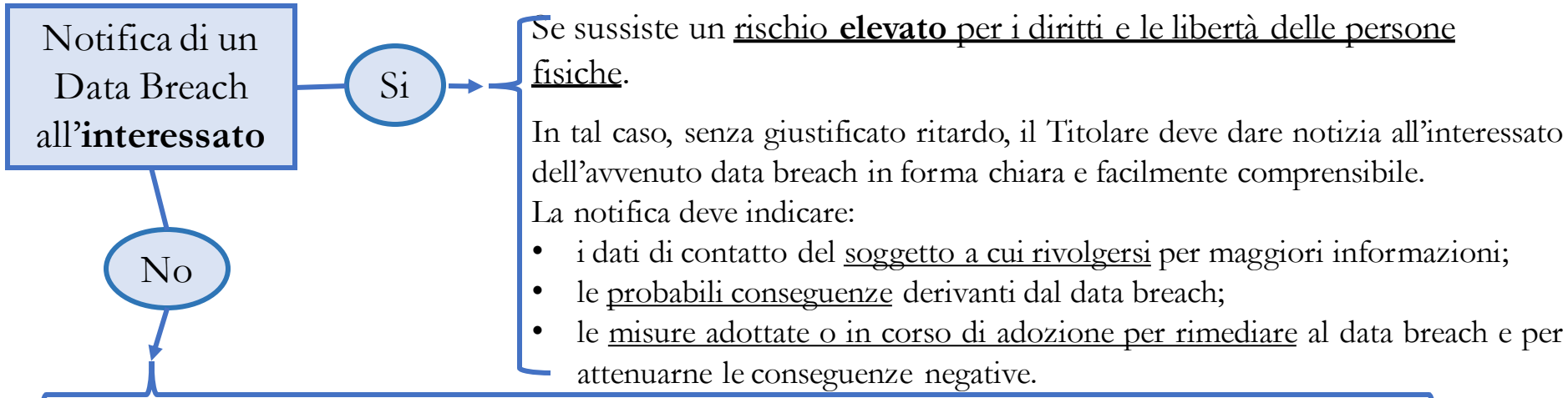
Qualora non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ingiustificato ritardo.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Accountability e approccio basato sul rischio: violazioni dei dati personali (data breach)

GDPR: art. 34 e considerando 86, 87 e 88

WP29 "Guidelines on Personal data breach notification under Regulation 2016/679" - Adottate 3 ottobre 2017, riviste 6 febbraio 2018



Regolamento UE e diritto del lavoro

Sistemi di monitoraggio sul posto di lavoro

TECNOLOGIE E STRUMENTI DI COMUNICAZIONE ELETTRONICA

- ✓ *Internet*
- ✓ *Posta elettronica*
- ✓ *Videosorveglianza*
- ✓ *Geolocalizzazione*
- ✓ *Social*

Art. 4 l.n. 300/1970 come modificato dall'art. 23 d.lgs. n. 151 del 2015

Parere 2/2017 sul trattamento dei dati nel posto di lavoro

Gruppo "Articolo 29" dell'8 giugno 2017

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Art. 4 l. 300/70 (Art. 23 d.lgs. 151/2015

Impianti audiovisivi e altri strumenti di controllo

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.(*)

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

_____

(*) Comma modificato dall'art. 5, comma 2 d.lgs.. 24 settembre 2016, n. 185

Strumenti di registrazione degli accessi e delle presenze

Art. 4, comma 2, l.n. 300 del 1970

"La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di **registrazione degli accessi e delle presenze**"

- ✓ Badge apri-porta
- ✓ Accessi aree riservate
- ✓ Accessi logici

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa

BADGE

- Il badge ad alta frequenza è uno strumento di controllo a distanza e non un semplice rilevatore di presenze (Cass. 17531 del 2017)
- Un badge elettronico idoneo a rilevare non solo la presenza ma anche le sospensioni, i permessi e le pause, ed a comparare nell'immediatezza i dati di tutti i dipendenti è uno strumento di controllo a distanza (Cass. 9904 del 2016)

Dati biometrici

Art. 2 septies d.lgs..n. 196 del 2003 (nuovo testo)

"7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo."

Posta elettronica ed internet

Provvedimento del Garante n. 303 del 13 luglio 2016

Con riferimento al servizio di posta elettronica e di navigazione web devono ritenersi come **strumenti di lavoro solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa, anche sotto il profilo della sicurezza**. A titolo esemplificativo possono essere considerati strumenti di lavoro il servizio di posta elettronica offerta ai dipendenti (mediante attribuzione di un account personale) e gli altri servizi della rete aziendale, fra cui anche il collegamento a siti internet. Costituiscono parte integrante di questi strumenti anche i sistemi e le misure che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete aziendale messa a disposizione del lavoratore

ESEMPI

- ✓ Sistemi di login per il corretto esercizio per il servizio di posta elettronica con conservazione al massimo di 7 giorni dei soli dati esteriori
- ✓ Sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete
- ✓ Sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Videosorveglianza

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento del garante aprile 2010

PRESUPPOSTI

liceità	rispetto delle norme sul controllo a distanza
necessità	conformazione dei programmi in modo da privilegiare dati anonimi
proporzionalità	scelta della dislocazione delle telecamere e delle modalità di ripresa, secondo il principio di pertinenza e non eccedenza

segue ….

Videosorveglianza

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Rapporto di lavoro

- Vietate riprese per verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione
- Rispetto della dignità e libertà del lavoratore ai sensi dell'art. 4 della legge 300 del 1970
- Applicazione delle procedure garantiste anche nell'ipotesi in cui le telecamere riprendano incidentalmente il lavoratore

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Videosorveglianza

Ministero del Lavoro e
delle Politiche Sociali

Nota n. 11241 - 1° giugno 2016

- L'installazione di un impianto di videosorveglianza non può avvenire antecedentemente, e quindi in assenza, di uno specifico accordo con i sindacati, o in mancanza, di autorizzazione amministrativa.
- La violazione dell'art. 4 non è esclusa dalla circostanza che tali apparecchiature siano solo installate ma non ancora funzionanti, né dall'eventuale preavviso dato ai lavoratori, né infine dal fatto che il controllo sia discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente.
- La condotta criminosa è rappresentata dalla mera installazione non autorizzata dell'impianto, a prescindere dal suo effettivo utilizzo.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Videosorveglianza

NOTA N. 4619 - 24 MAGGIO 2017

- La procedura autorizzativa dell'ITL è successiva al mancato accordo verificatori in sede aziendale con gli organismi sindacali interni
- l'autorizzazione rilasciata dall'ITL può essere sostituita da un successivo accordo sindacale
- le organizzazioni sindacali deputate al raggiungimento dell'accordo sono la RSU o la RSA e le organizzazioni sindacali comparativamente più rappresentative a livello nazionale
- l'accordo viene ritenuto valido se raggiunto con la sola maggioranza della RSA (nota del Ministero del Lavoro n. 2975 del 5 dicembre 2015)
- le intese raggiunte ex art. 8, comma 2, della legge n. 148/2011 in materia di video sorveglianza debbono trovare il proprio fondamento negli obiettivi indicati al comma 1. Gli accordi, derogatori rispetto art. 4, debbono garantire il rispetto della Costituzione, delle norme comunitarie e delle convenzioni internazionali in materia di lavoro

Videosorveglianza

Circolare n. 5 - 19 febbraio 2018

Installazione e utilizzazione di impianti audiovisivi e di altri strumenti di controllo

1) ISTRUTTORIA DELLE ISTANZE PRESENTATE PER L'INSTALLAZIONE DI IMPIANTI DI VIDEOSORVEGLIANZA

- ✓ l'Ispettorato deve valutare l'effettiva sussistenza delle ragioni che giustificano l'autorizzazione (ragioni organizzative e produttive, sicurezza del lavoro, tutela del patrimonio aziendale)
- ✓ in tali casi, fermo il principio per cui, di norma, la ripresa dei lavoratori dovrebbe avvenire in via incidentale e con carattere di occasionalità, l'impianto può anche inquadrare direttamente i lavoratori, senza limitazioni quali l'angolo di ripresa della telecamera o l'oscuramento del volto del lavoratore

Videosorveglianza

Circolare n. 5 - 19 febbraio 2018

2) TUTELA DEL PATRIMONIO AZIENDALE

- ✓ nessun problema per dispositivi collegati ad impianti antifurto purché entrino in funzione in assenza dei lavoratori
- ✓ rispetto dei principi di legittimità, determinatezza delle finalità, proporzionalità, correttezza e non eccedenza per dispositivi operanti in presenza di lavoratori ➔ gradualità del monitoraggio – esclusione di controlli invasivi

3) TELECAMERE

- ✓ l'accesso da postazioni remote alle immagini "in tempo reale" può essere autorizzato in casi eccezionali e motivati
- ✓ l'accesso a immagini registrate deve essere tracciato; conservazione per un tempo limitato (non inferiore a 6 mesi); superato il sistema della "doppia chiave fisica o logica"
- ✓ autorizzazione (o accordo sindacale) anche per l'installazione in locali "privati" ad accesso saltuario o occasionale dei lavoratori

Geolocalizzazione

Circolare n. 2 - 7 novembre 2016

Apparecchi di localizzazione satellitale gps montati su autovetture aziendali

- Se "**elementi aggiunti**" per esigenze assicurative, produttive o di sicurezza del lavoro richiedono l'accordo sindacale o, in mancanza, l'autorizzazione amministrativa, ex art. 4, 1° comma.

- In casi particolari, se installati per consentire la concreta ed effettiva prestazione lavorativa (che non può essere resa senza tali strumenti) o se richiesta da specifiche normative di legge o regolamentari (esempio per trasporto valori oltre 1.5 milioni di euro) **costituiscono strumenti di lavoro** ex art. 4, 2° comma.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Localizzazione di dispositivi smartphone e tablet

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento garante n. 505 del 30 novembre 2017

- Sistema tecnologico che consente la localizzazione geografica di dispositivi aziendali forniti ai dipendenti allo scopo di certificare ai clienti l'effettuazione delle attività di controllo sulla qualità di distribuzione del materiale pubblicitario.

- Sistema non direttamente proporzionato all'esecuzione della prestazione lavorativa: accordo sindacale.
- Necessità di posizionare un'icona che indichi l'attivazione della localizzazione.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Geolocalizzazione

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento n. 138 – 16 marzo 2017

Localizzazione geografica dei veicoli utilizzati da una compagnia di servizi idrici

- ottimizzazione richiesta di intervento e emergenze
- innalzamento delle condizioni di sicurezza sul lavoro dei dipendenti
- corretta manutenzione dei veicoli
- tutela del patrimonio aziendale
- calcolo dei tempi di lavoro effettivo
- gestione di incidenti stradali e sanzioni per violazione del codice della strada

Installazione legittima per le finalità indicate nel rispetto della privacy dei lavoratori

Il sistema può consentire il controllo a distanza dei lavoratori e necessita di previo accordo sindacale o, in mancanza, di autorizzazione amministrativa

segue ….

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Geolocalizzazione

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento n. 138 – 16 marzo 2017

Vanno definite le modalità di raccolta, di elaborazione e conservazione dei dati di geolocalizzazione e degli altri dati personali, differenziando le tutele in base alle singole finalità perseguite.

Ad esempio:

- regolare tenuta del libro unico del lavoro ➔ conservazione per 5 anni
- contestazione violazioni amministrative ➔ conservazione max 90 gg. (ovvero il tempo previsto per la notificazione del verbale di contestazione)
- cancellazione o anonimizzazione automatica dei dati al termine del periodo di conservazione
- trattamento dei dati sui percorsi in forma aggregata o anonima per finalità statistiche o di programmazione del lavoro
- adozione di misure di sicurezza e accesso ai dati dei soli incaricati
- adeguata informazione ai dipendenti

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Smartphone e rilevazione delle presenze

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento n. 350 – 8 settembre 2016

- Applicazione – contenente una funzionalità di localizzazione geografica – sul dispositivo smartphone dei dipendenti, preordinata all'effettuazione della timbratura del cartellino e alla rilevazione delle presenze

legittimità

- ✓ alternatività del sistema
- ✓ risparmio gestione; semplificazione ed incremento dell'efficienza e della certezza della rilevazione
- ✓ cancellazione di tutti i dati: solo dato relativo alla presenza nella sede di lavoro
- ✓ temporaneità della conservazione
- ✓ informazione ai dipendenti
- ✓ configurazione che renda sempre visibile sullo schermo l'icona indicante che la funzionalità è attiva

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

PROFILO SANZIONATORIO

Tipo di violazione	Tipo di sanzione
Installazione di impianti e strumenti non per la sicurezza del lavoro e per la tutela del patrimonio aziendale (cioè finalizzati esclusivamente per il controllo dell'attività dei lavoratori) (legge n. 300/1970, art. 4, comma 1)	-Ammenda da € 154 a € 1.549 o arresto da 15 giorni ad un anno (legge n. 300/1970, art. 38, comma 1) - Ammenda e arresto applicate congiuntamente (nei casi più gravi) (legge n. 300/1970, art. 38, comma 2) - Ammenda aumentabile fino al quintuplo (in base alle condizioni economiche del reo) (legge n. 300/1970, art. 38, comma 3) - Pubblicazione della sentenza di condanna (nei casi più gravi).0 (legge n. 300/1970, art. 38, comma 4)
Installazione di impianti e strumenti per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori senza accordo sindacale o autorizzazione delle strutture periferiche o centrale del Ministero del lavoro (legge n. 300/1970, art. 4, comma 1)	
Mancata informazione dei lavoratori (legge n. 300/1970, art. 4, comma 3)	
Mancato coinvolgimento delle rappresentanze sindacali (condotta antisindacale) (legge n. 300/1970, art. 4, comma 1)	Ordine di cessazione del comportamento antisindacale (legge n. 300/1970, art. 28
Inosservanza del provvedimento del giudice (di cessazione del comportamento antisindacale) (Cod. pen., art. 650)	- Arresto fino a tre mesi o ammenda fino a € 206 (Cod. pen., art. 650)

Data Breach Notification – Art. 33

Nel caso in cui si verifichi una violazione di dati personali, il Titolare del Trattamento ha l'Obbligo di Notifica, che dovrà essere eseguito sia ai diretti interessati, che all'Autorità Garante per la protezione dei dati personali, entro ~~24 ore~~ 72 ore. Attualmente in Italia tale obbligo trova applicazione per le sole organizzazioni che forniscono servizi di comunicazione elettronica.

Soggetti Interessati

Autorità Garante

~~Conservazione Registro Pubblico delle tipologie di violazioni notificate~~

La decorrenza delle 72 ore parte dal momento in cui il Titolare viene a conoscenza della violazione, a meno che sia improbabile che essa presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora non siano rispettate tali tempistiche, la notifica all'Autorità Garante va corredata da una giustificazione motivata.

Data Breach Notification – Art.33

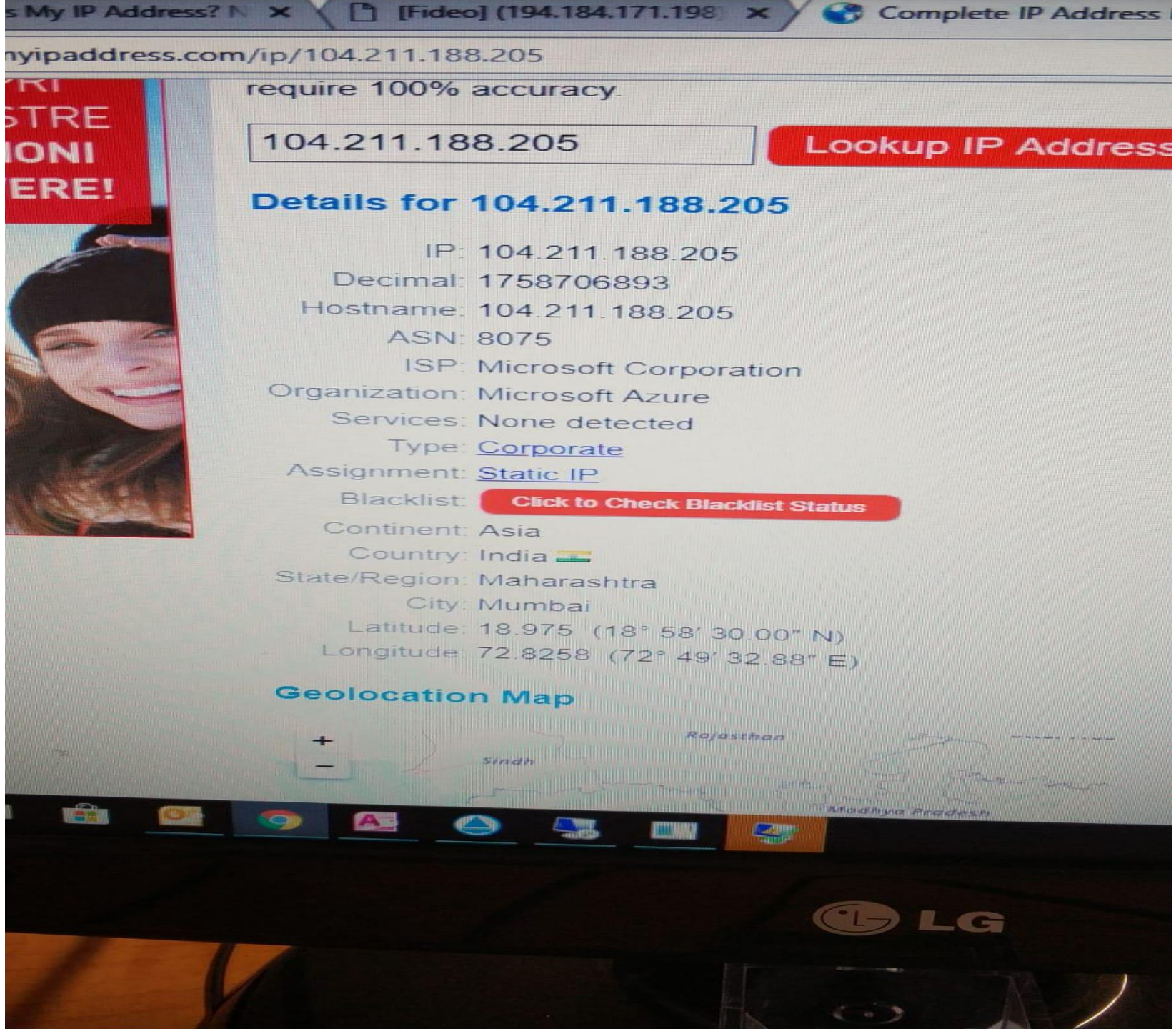
La comunicazione all'Interessato non è richiesta nei casi di:

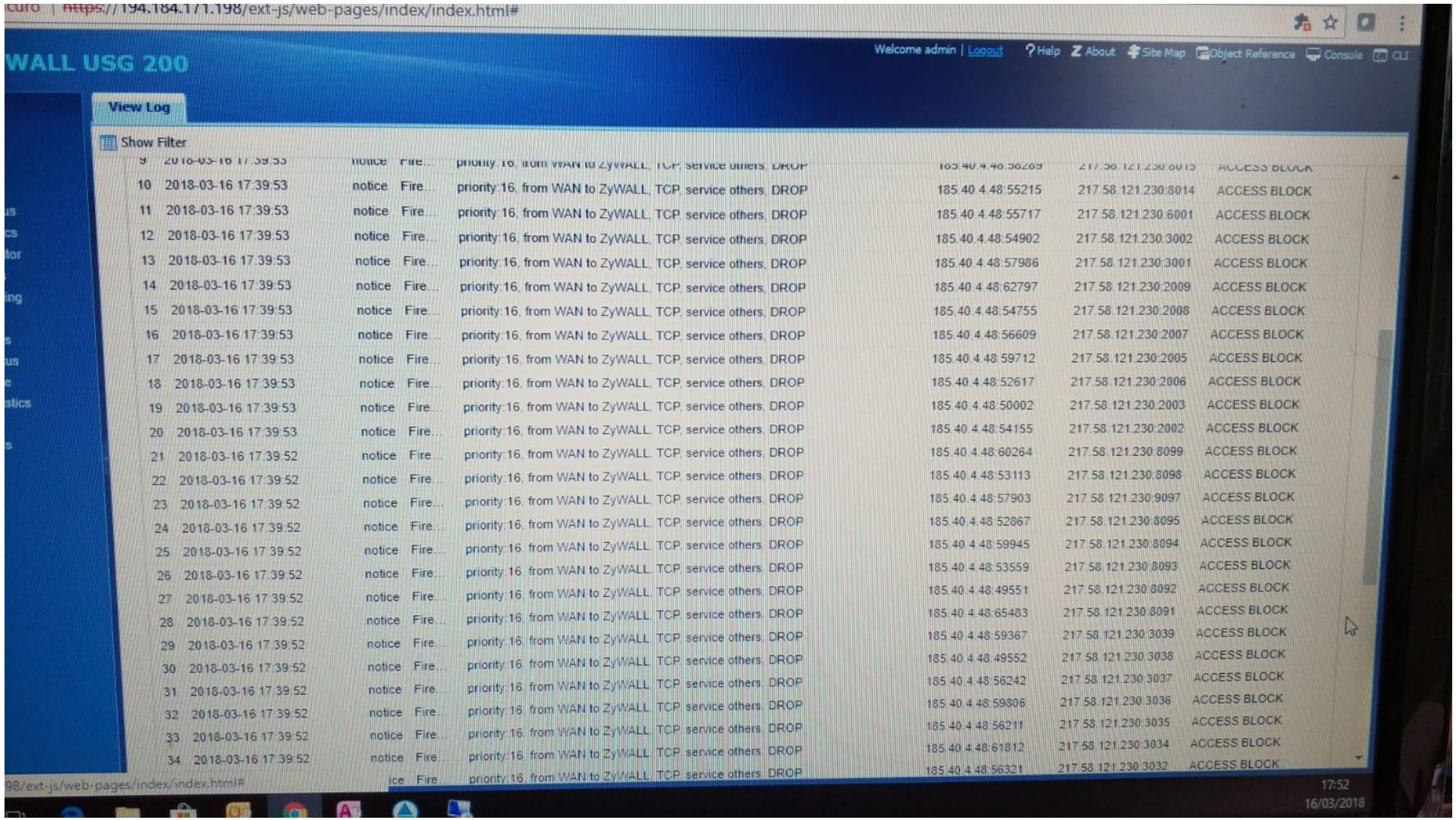
Utilizzo di misure tecniche e organizzative adeguate per rendere i dati incomprensibili ai soggetti non autorizzati (cifratura)

Successiva adozione di misure atte a scongiurare il sopraggiungere di rischi per i diritti e le libertà degli interessati

Comunicazione particolarmente difficoltosa o onerosa per il Responsabile

In questo caso occorre procedere a comunicazione pubblica o misura simile


s My IP Address? N
[Fideo] (194.184.171.198
Complete IP Address
nyipaddress.com/ip/104.211.188.205
require 100% accuracy.
104.211.188.205
Lookup IP Address
Details for 104.211.188.205
IP: 104.211.188.205
Decimal: 1758706893
Hostname: 104.211.188.205
ASN: 8075
ISP: Microsoft Corporation
Organization: Microsoft Azure
Services: None detected
Type: Corporate
Assignment: Static IP
Blacklist: Click to Check Blacklist Status
Continent: Asia
Country: India
State/Region: Maharashtra
City: Mumbai
Latitude: 18.975 (18° 58′ 30.00″ N)
Longitude: 72.8258 (72° 49′ 32.88″ E)
Geolocation Map
Rajasthan
Sindh
Madhya Pradesh
LG



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Data Protection Officer – Art. 37

Il Data Protection Officer, che potrà essere interno od esterno all'organizzazione, avrà il compito di progettare e mantenere un sistema organizzato e sicuro di gestione dei dati personali. Tale figura dovrebbe poter adempiere alle proprie funzioni in maniera indipendente.

Per chi sarà Obbligatorio?

Pubblica Amministrazione
Molto più di un'icona.

Pubbliche Amministrazioni

~~Grandi Aziende Private (oltre 250 dipendenti)~~

In Caso di Trattamento di Dati di ~~più di 5.000~~ Interessati su larga scala

In Caso di Trattamento di Dati Particolari su larga scala

Facoltatività per ciascuno Stato membro di introdurre la figura del DPO come obbligatoria.

Enti pubblici o gruppi d'imprese possono nominare un unico DPO per più stabilimenti/autorità.

I Compiti del DPO – Art. 39

Informare e consigliare Titolare, Responsabili e dipendenti

Sorvegliare l'attuazione e l'applicazione del Regolamento

Sorvegliare l'attuazione e l'applicazione delle politiche aziendali

~~Garantire la conservazione del Registro delle Attività di Trattamento~~

~~Controllare che le violazioni dei dati siano notificate~~

Verificare e fornire un parere sulla valutazione d'impatto

Cooperare con l'Autorità di controllo

Fungere di punto di contatto tra l'Autorità e gli Interessati

Il DPO opera considerando i rischi inerenti al trattamento, tenendo conto della relativa natura, campo di applicazione, contesto e finalità.

Le Competenze del DPO – Art. 37

Conoscenza Specialistica della Normativa

Conoscenza delle Pratiche in materia di Protezione dei Dati

Adempiere ai Compiti dell' Art. 39

Padronanza Requisiti Tecnici

Specifica Conoscenza del Settore

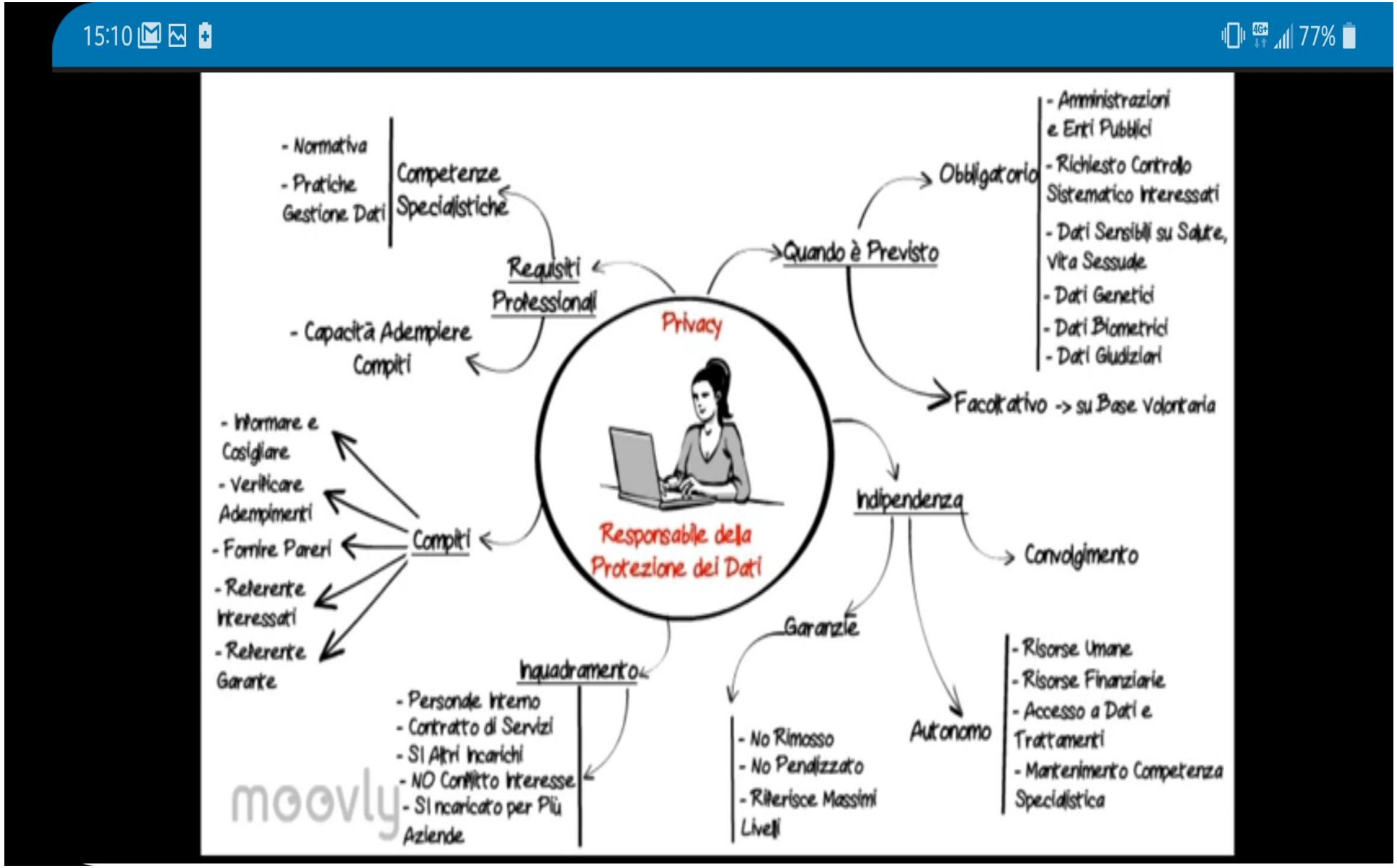
Analisi, Audit e Consultazioni

Collaborazione e Spiccate Capacità Relazionali

Formazione Avanzata Specializzata

Questi requisiti minimi era presenti in modo esplicito soltanto nel testo del Parlamento Europeo (75 bis). Nel testo definitivo si fa riferimento solo alle tre competenze riportate in alto.

Il DPO è una figura autonoma e indipendente dall'organizzazione e riferisce direttamente al vertice gerarchico.



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

VIDEOREGISTRAZIONE
Legge 20 maggio 1970, n. 300

- Informativa
- Soggetti preposti e misure di sicurezza
- Durata dell'eventuale conservazione
- Diritti degli interessati
- VALUTAZIONE DI IMPATTO (DPIA)

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

VIDEOSORVEGLIANZA
Legge 20 maggio 1970, n. 300 art. 4/Provv. Garante 08/04/2010

- ACCORDO TRA DATORE DI LAVORO E RAPPRESENTANTE DEI LAVORATORI

- AUTORIZZAZIONE PREVENTIVA ISPETTORATO PROVINCIALE DEL LAVORO

- ACCORDO CON ISPETTORATO DI PALERMO PER OPERARE UNA "SANATORIA"
  - ISTANZA CON RACCOMANDATA A/R E MARCA DA BOLLO DA € 14,62

- La verifica ispettiva dell'Ispettorato Provinciale del Lavoro verterà soltanto sul tema Videosorveglianza e verificherà se:
  - Le telecamere sono correttamente installate;
  - Il sistema di registrazione è custodito in un armadio metallico chiuso con doppia serratura a chiave e le chiavi siano in possesso del datore di lavoro e di un lavoratore;

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

VIDEOREGISTRAZIONE
Legge 20 maggio 1970, n. 300 art. 4/Provv. Garante 08/04/2010

- L'ispettore inoltre, a fine verifica, su verbale, richiede:
  - Un'altra marca da bollo da 14, 62 euro;
  - relazione tecnica riguardo la tipologia delle attrezzature utilizzate (telecamere e registratore);
  - un elaborato grafico (planimetria) con la disposizione delle telecamere (con il cono ottico e del registratore);
  - Documentazione relativa agli adempimenti di cui al D.Lgs 81/08 (autocertificazione)
  - Documentazione relativa agli adempimenti di cui al DM 37/08 ex Legge 46/90;
  - Denuncia dell'impianto di Terra.
  - Regolamento sulla Videosorveglianza;

VIDEOREGISTRAZIONE
Legge 20 maggio 1970, n. 300 art. 4/Provv. Garante 08/04/2010

- Sentenza Cassazione V Sez.Penale n. 20722/2010

- Legittima i controlli di un'agenzia investigativa contro attività fraudolente del dipendente di una ditta.
- Nella vicenda era stata filmata, a sua insaputa, una cassiera di un bar che rubava dalla cassa del bar stesso.

Quando l'uso delle telecamere sul lavoro è legittimo?

Spiare con una telecamera i dipendenti è reato, l'uso della videosorveglianza in azienda è consentito solo per una delle tre seguenti finalità:

- **esigenze organizzative e produttive**: si pensi alla necessità di riprendere un macchinario per verificare che questo funzioni correttamente e finisca un ciclo di produzione per iniziarne un altro; oppure a una telecamera posta sull'uscio del negozio per vedere se entrano clienti e riceverli;

- **tutela della sicurezza del lavoro**: si pensi a una telecamera in un ufficio postale o in una banca per dissuadere i ladri dalla tentazione di fare una rapina

- **tutela del patrimonio aziendale**: si pensi a una telecamera posta nei vari reparti del supermercato per evitare che qualche cliente – o qualche dipendente stesso – prelevi della merce senza pagarla.

.

Telecamere con immagini visibili dallo smartphone

La circolare n. 5 INL si sofferma poi sui nuovi strumenti che consentono di verificare, in tempo reale, da un normale cellulare, il raggio di azione e le riprese delle telecamere. Ciò è legittimo – dice l'INL – solo in casi eccezionali debitamente motivati». Prosegue la circolare precisando che l'accesso alle immagini registrate va tracciato in modo che i relativi «log di accesso» siano conservati per un periodo non inferiore a sei mesi.

Non è, invece, più posto come requisito l'uso di un sistema a **«doppia chiave fisica e logica**

- Whistleblowing

- e interconnessioni con la normativa sulla protezione dei dati personali

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

SCHE) di attuazione della Direttiva UE 2019/1937

Articolo 14

ogni trattamento dei dati personali previsto dal decreto, deve essere effettuato a norma del regolamento (UE) 2016/679 (GDPR),
del decreto legislativo 30 giugno 2003, n. 196 (Codice Privacy)
e del decreto legislativo 18 maggio 2018, n. 51.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

IL PARERE DEL GARANTE PRIVACY

Parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'unione (cd. direttiva whistleblowing) -11 gennaio 2023 [9844945]

GPDP

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

ai sensi dell'articolo 36, paragrafo 4, del Regolamento, esprime **parere favorevole** sul proposto schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre ante la protezione delle persone che segnalano violazioni d unione e disposizioni riguardanti la protezione delle pers alano violazioni delle disposizioni normative nazionali.

IL PRESIDENTE Stanzione

Roma, 7 7 gennaio 2023

IL RESIDENTE Stanzione

IL RELATORE Scorza

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

- DISCIPLINA DI SETTORE

Una delle “norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo **al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro**” previste dall'art. 88, par. 1, del GDPR

DECRETO LEGISLATIVO 10 marzo 2023, n. 24

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

WHISTLEBLOWING E PRINCIPI PRIVACY

Art. 12	**le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse (principio di finalità, art. 5, par.1, lett. b del GDPR);**	
Art. 13	i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non devono essere raccolti o, se raccolti accidentalmente, devono essere cancellati immediatamente (principio di minimizzazione dei dati, art. 5, par. 1, lett. c del GDPR);	
Art. 14	la conservazione delle segnalazioni, interne ed esterne, e della relativa documentazione deve essere limitata al tempo necessario al trattamento della segnalazione (principio di limitazione della conservazione, art. 5, par. 1, lett. e del GDPR) e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione	

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

WHISTLEBLOWING E PRINCIPI PRIVACY

Art. 13	**fornire idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679**	

Rendere *ex ante* ai possibili interessati (ad es. segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) **un'informativa sul trattamento dei dati personali** mediante la pubblicazione di documenti informativi ad esempio tramite sito web, piattaforma, informative brevi in occasione dell'utilizzo degli altri canali previsti dal decreto.

Nella fase di acquisizione della segnalazione e della eventuale successiva istruttoria **non** devono invece essere fornite informative *ad hoc* ai vari **soggetti interessati diversi dal segnalante**. Laddove all'esito dell'istruttoria sulla segnalazione si avvii un procedimento nei confronti di uno specifico soggetto segnalato, a quest'ultimo va naturalmente resa un'informativa *ad hoc*.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

ESERCIZIO DEI DIRITTI

- «La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, **non possono esercitare** - per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento).

Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante. (Linee Guida ANAC)

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

ECLAMO AL GARANTE PRIVACY

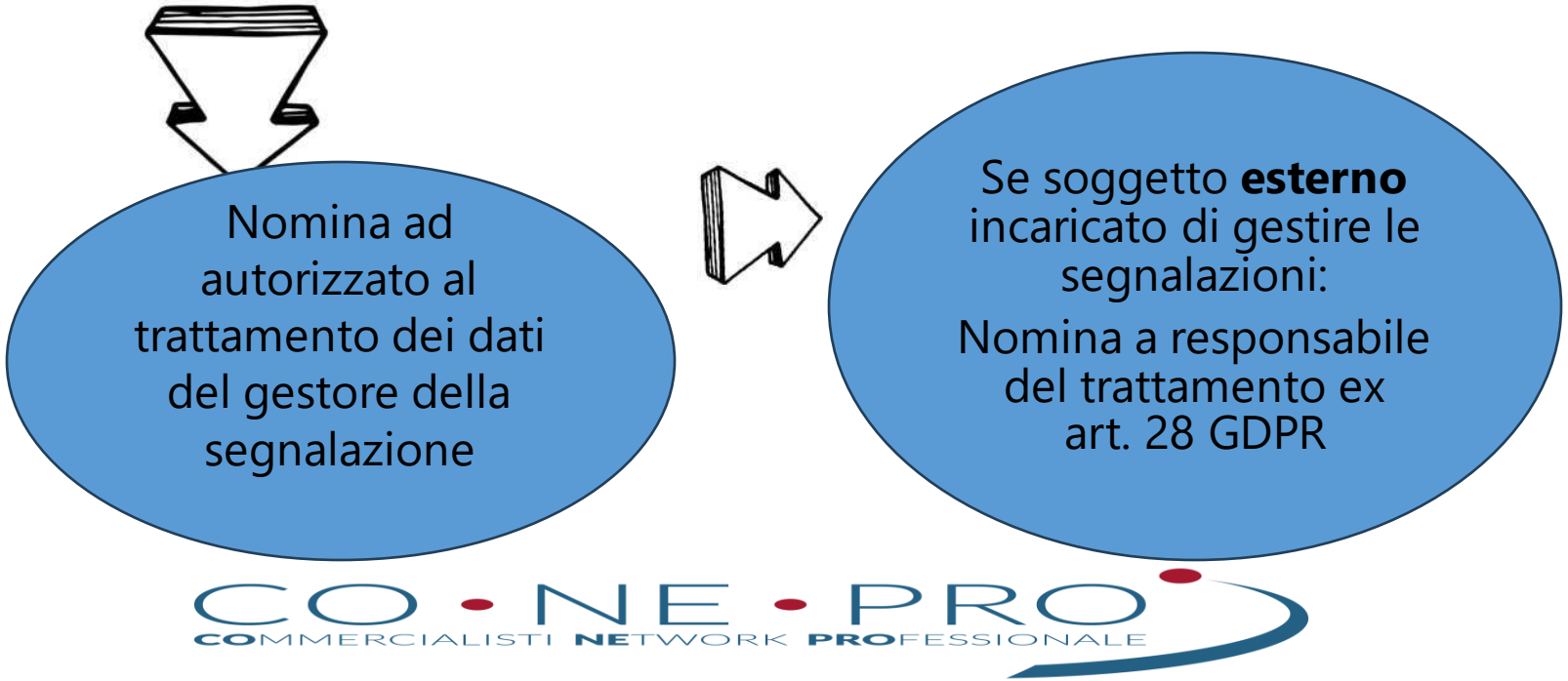
•Al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di **rivolgersi al titolare** del trattamento e, in assenza di risposta da parte di quest'ultimo, di **proporre reclamo al Garante** della protezione dei dati personali.

•

(Linee Guida ANAC)

WHISTLEBLOWING E PRINCIPI PRIVACY

Art. 12	**l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli artt. 29 e 32, par. 4, del GDPR e dell'art. 2-quaterdecies del Codice Privacy (principio di riservatezza, art. 5, par. 1, lett. f del GDPR).**	

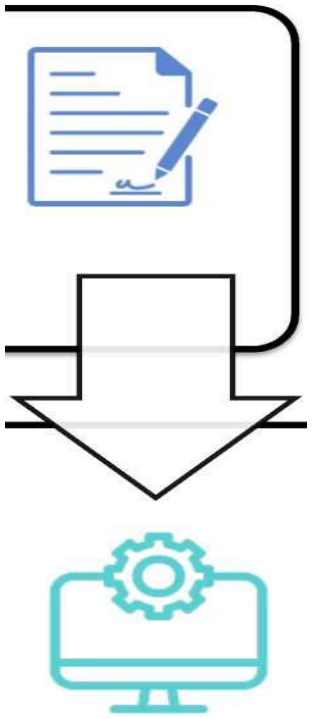


CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

RAPPORTI CON I SOGGETTI ESTERNI

Disciplinare il rapporto con eventuali **fornitori esterni** che trattano dati personali per loro conto come previsto dall'articolo 28 GDPR stipulando il relativo **contratto di nomina**.

Fornitori della **piattaforma di whistleblowing**, del servizio di **hosting**, etc...



CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Question Time

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Dr. DAVIDE CANDIA

- Dottore Commercialista – Revisore Legale Dei Conti - Organismo di Vigilanza ex D.lgs 231/2001 - consulente Privacy - Data Protection Officer
- E-mail: studiocandiadavide@gmail.com
- Tel: 0919740112
- Fax: 0917657642
- Cell: 3281926806
- Linkedin:http://it.linkedin.com/pub/davidecandia/52/601/b3b

CO•NE•PRO
COMMERCIALISTI NETWORK PROFESSIONALE

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE