“Regolamento Europeo”
GENERAL DATA PROTECTION REGULATION
GDPR
Regolamento UE 2016/679

DATA BREACH NOTIFICATION
Art. 33 GDPR 679/2016

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.

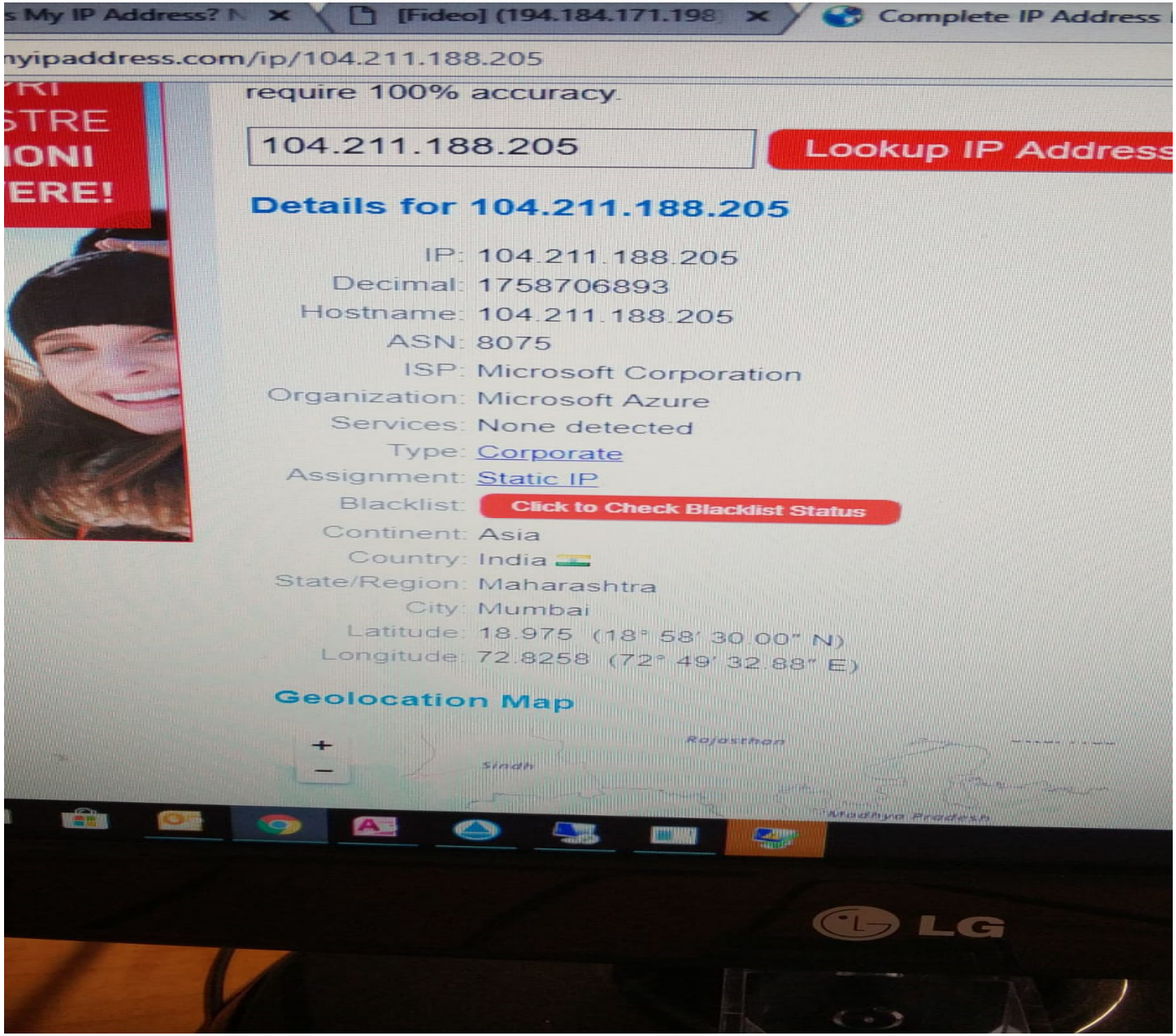
Il GDPR adotta taluni "strumenti" al fine di rafforzare la tutela dei dati e la responsabilizzazione del Titolare e del Responsabile del trattamento:

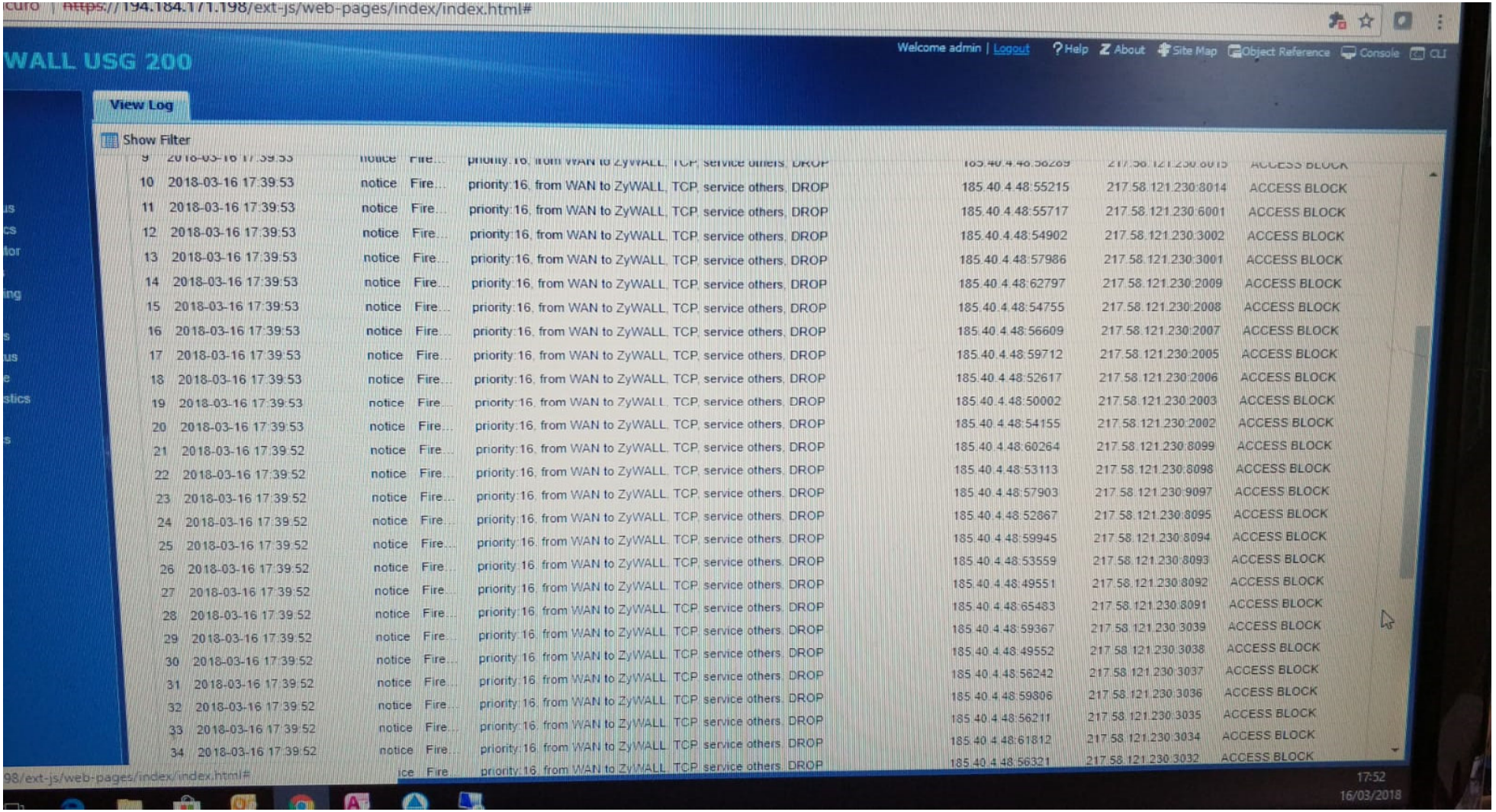
- sancisce il principio di *accountability* (Art. 5, par. 2);
- sancisce i principi della *privacy by design* e della *privacy by default*;
- Prevede la tenuta del Registro dei trattamenti;
- richiede d'implementare adeguate misure di sicurezza, tenendo in considerazione le tipologie di operazioni svolte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

• Obbligo della Notificazione della violazione e furto dei Dati

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.

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


My IP Address?
[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
LG



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.

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.

Allegati:

Delivery Note - AWD 72703432141- 009 2203960288.pdf.gz 348 kB

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.
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>

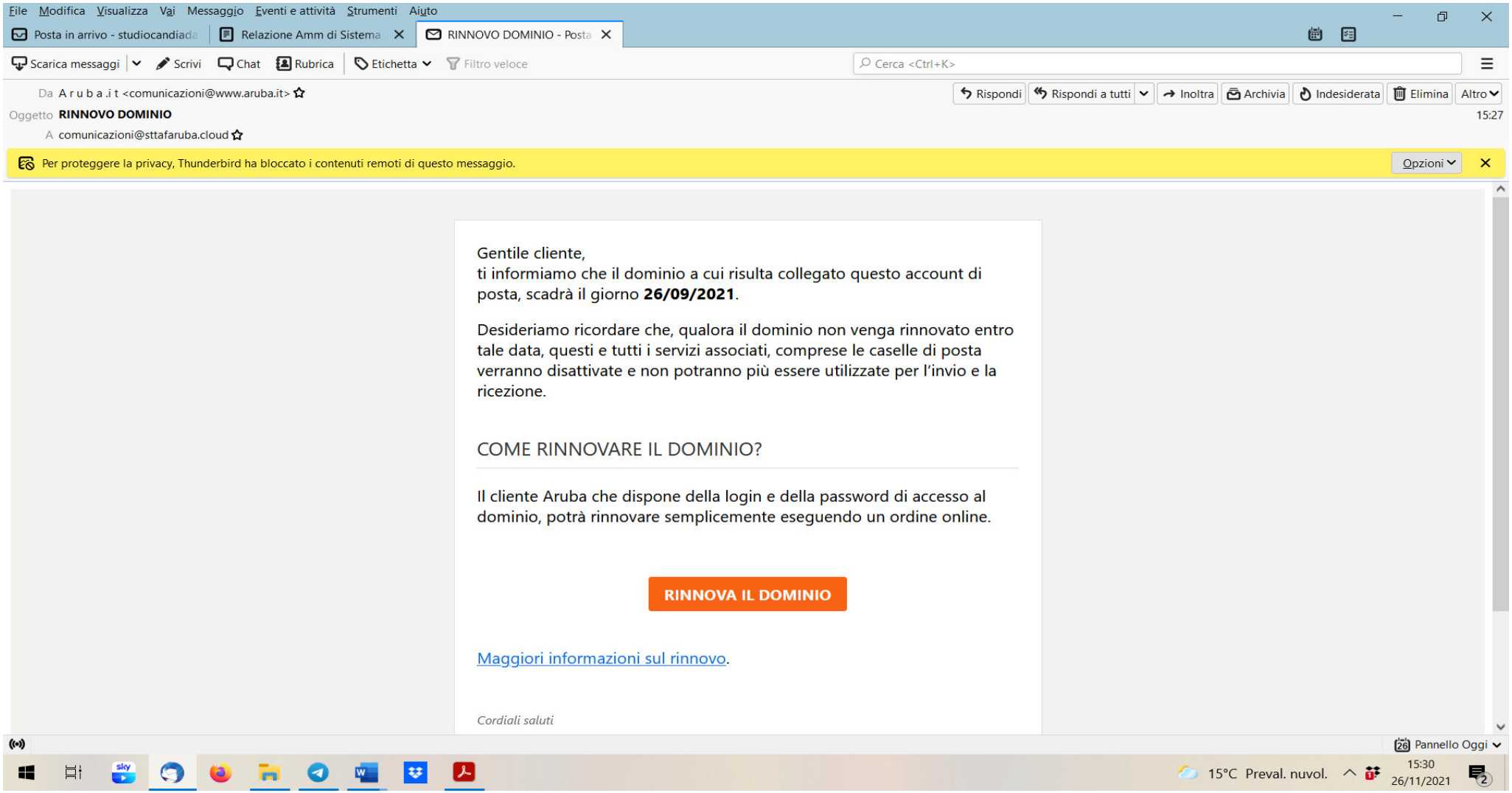
Gentile cliente,

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

Accesso al rimborso

Dopo aver ricevuto il modulo [illegible]errà addebitato il rimborso
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

SAMSUNG 4K ULTRA HD

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

PRO 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

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».

Il Titolare deve 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:

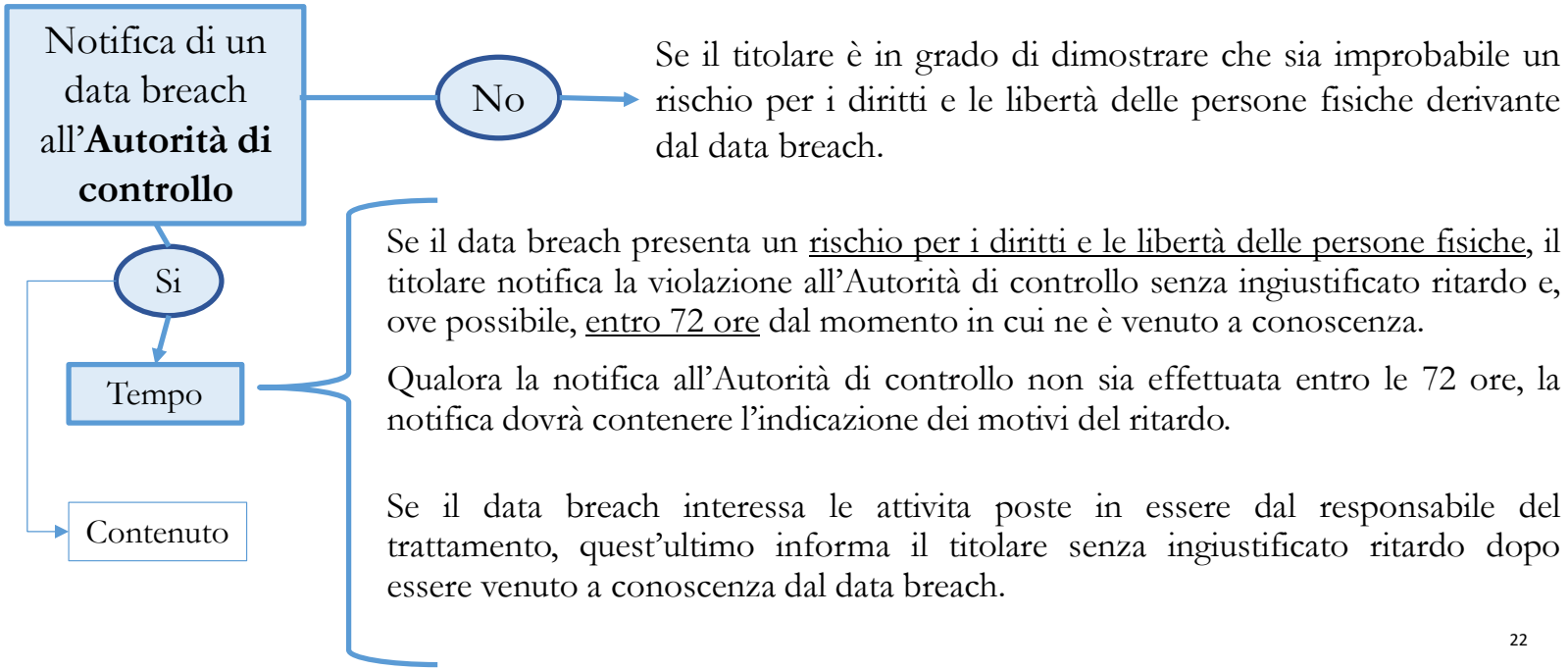
- perdita di controllo dei dati personali;
- limitazione dei diritti;
- discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati protetti da segreto professionale;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

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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



Se il titolare è in grado di dimostrare che sia improbabile un rischio per i diritti e le libertà delle persone fisiche derivante dal data breach.

Se il data breach presenta un rischio per i diritti e le libertà delle persone fisiche, il titolare notifica la violazione all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza.

Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, la notifica dovrà contenere l'indicazione dei motivi del ritardo.

Se il data breach interessa le attivita poste in essere dal responsabile del trattamento, quest'ultimo informa il titolare senza ingiustificato ritardo dopo essere venuto a conoscenza dal data breach.

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

Notifica di un data breach all'**Autorità di controllo**

Si

Tempo

Contenuto

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

Notifica di un Data Breach all'interessato

Si

Se sussiste un rischio **elevato** per i diritti e le libertà delle persone fisiche.

In tal caso, senza giustificato ritardo, il Titolare deve dare notizia all'interessato dell'avvenuto data breach in forma chiara e facilmente comprensibile.
La notifica deve indicare:

- 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.

No

- se il titolare aveva adottato le misure tecniche e organizzative adeguate di protezione con riferimento ai dati oggetto del data breach;
- se il titolare dopo la violazione ha adottato misure atte a scongiurare un rischio elevato per i diritti e libertà dell'interessato derivante dal data breach;
- se la notifica richiederebbe uno sforzo sproporzionato per il titolare. In tal caso, si adottato modalità alternative per dare notizia dell'avvenuto data breach (es. comunicazione pubblica).

UniCredit

Milano, 28.10.2019

0053

99999

[redacted]

PLF61JAVASY03894C050

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.

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.

VIDEOREGISTRAZIONE
Legge 20 maggio 1970, n. 300

recepito dall'art. 114 del decreto legislativo n. 196/2003

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

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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

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

- ACCORDO SINDACACALE TRA DATORE DI LAVORO E LAVORATORI

- AUTORIZZAZIONE PREVENTIVA ISPETTORATO PROVINCIALE DEL LAVORO

- RICHIESTA C/O ISPETTORATO PROVINCIALE DEL LAVORO IN “SANATORIA”

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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

- La pratica prevede:
  - Istanza su modello PDF modificabile
  - 2 marche 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);
  - Informativa videosorveglianza firmata da tutti i dipendenti;
  - Solo per l'ISPL di Palermo il verbale di nomina tra i lavoratori del Responsabile delle Immagini;
  - **La verifica dell'Ispettorato Provinciale del Lavoro non è più contemplata.**

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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.

.

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Telecamere con immagini visibili dallo smartphone

La circolare n. 5 INL (Ispettorato Nazionale del Lavoro) 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**

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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)

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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."

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

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 con cancellazione dei META DATI dopo 7 Giorni
- ✓ 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

Provvedimento del 21 dicembre 2023 - Documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" [9978728]

Scheda

Doc-Web
9978728

Data
21/12/23

Argomenti

Misure di sicurezza | e-mail | Lavoro pubblico | Cloud

Tipologie

Deliberazione

VEDI ANCHE Newsletter del 6 febbraio 2024

METADATO

dal greco antico μετὰ?, "oltre, dopo, per mezzo" e dal latino *datum*, "informazione" - plurale: *data*, lett. "(dato) per mezzo di un (altro) dato") è un dato che descrive una qualche proprietà di un altro dato.

In senso lato è un'informazione a proposito di un'altra informazione.

COSA CANCELLARE? ORA, DATA, PROVENIENZA DATI REALATIVI ALLA TRACCIABILITA', TRACCIATI RECORD ETC

CO • NE • PRO
COMMERCIALISTI NETWORK PROFESSIONALE

Geolocalizzazione

Circolare n. 2 - 7 novembre 2016

Apparecchi di localizzazione satellitare 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

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)

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