Tutela della privacy

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

Dr. Davide Candia
Dr. Francesco La Franca

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


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

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

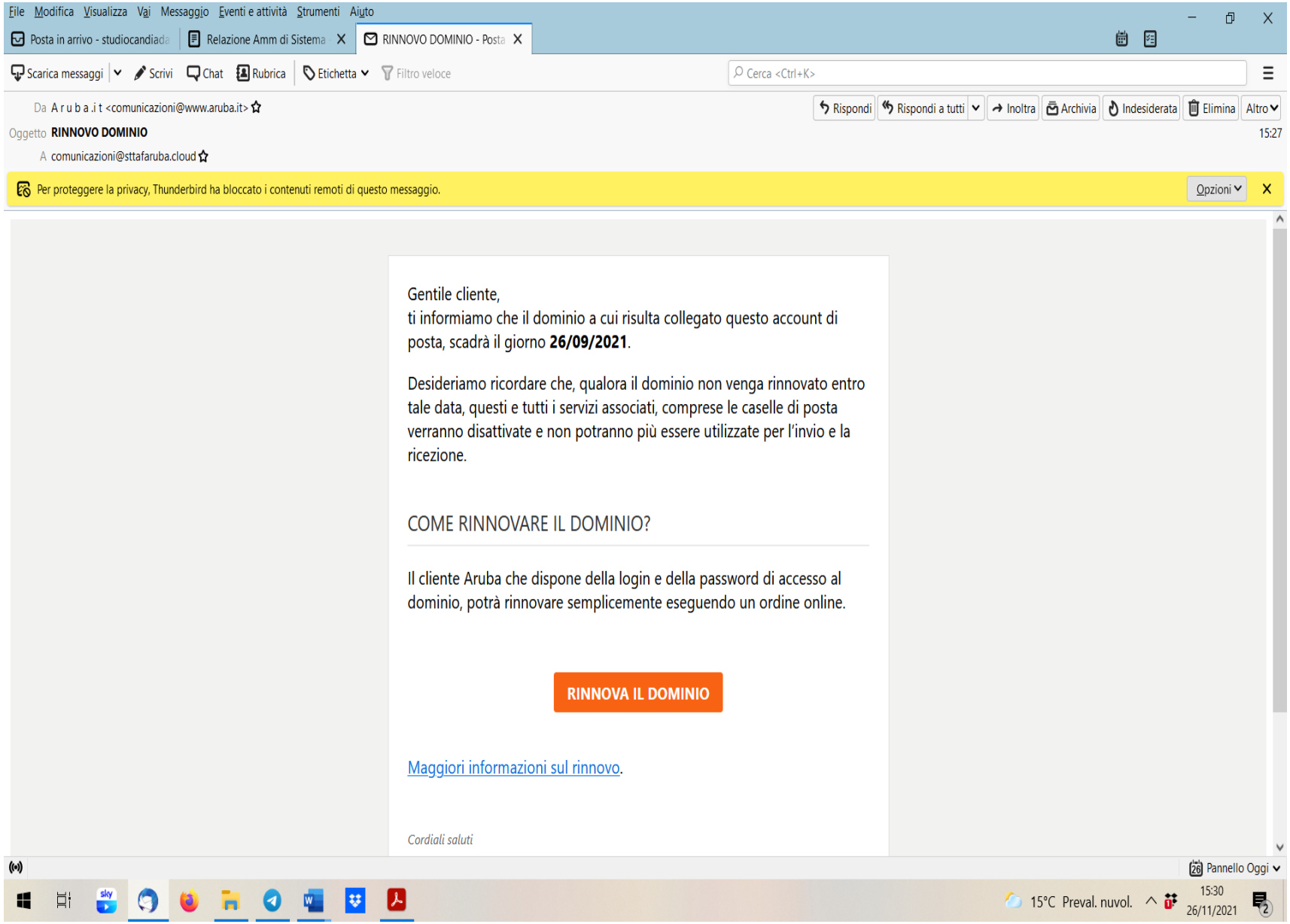
Oggetto: Avviso di rimborso!
Mittente: "Agenzia delle Entrate" <info@agenziadelleentrat.it>
Data: 17/02/2021, 03:58
A: "rpd@clinicacandela.it" <rpd@clinicacandela.it>

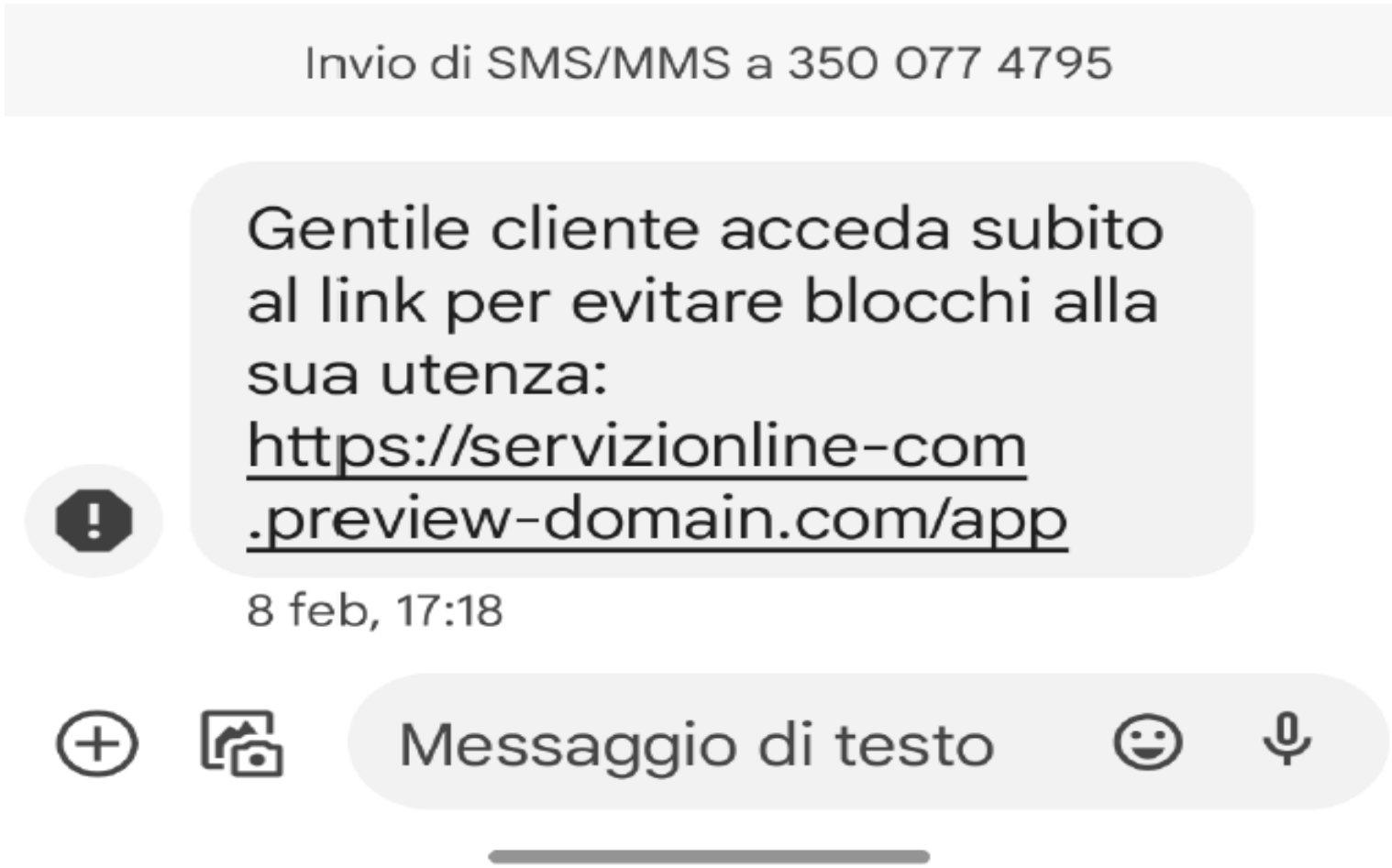
Gentile cliente,

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


File Modifica Visualizza Vai Messaggio Eventi e attività Strumenti Aiuto
Posta in arrivo - studiocandiada
Relazione Amm di Sistema
RINNOVO DOMINIO - Posta
Scarica messaggi
Scrivi
Chat
Rubrica
Etichetta
Filtro veloce
Cerca <Ctrl+K>
Da A r u b a .i t <comunicazioni@www.aruba.it>
Oggetto RINNOVO DOMINIO
A comunicazioni@sttafaruba.cloud
Rispondi
Rispondi a tutti
Inoltra
Archivia
Indesiderata
Elimina
Altro
15:27
Per proteggere la privacy, Thunderbird ha bloccato i contenuti remoti di questo messaggio.
Opzioni
Gentile cliente,
ti informiamo che il dominio a cui risulta collegato questo account di posta, scadrà il giorno 26/09/2021.
Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e non potranno più essere utilizzate per l'invio e la ricezione.
COME RINNOVARE IL DOMINIO?
Il cliente Aruba che dispone della login e della password di accesso al dominio, potrà rinnovare semplicemente eseguendo un ordine online.
RINNOVA IL DOMINIO
Maggiori informazioni sul rinnovo.
Cordiali saluti
Pannello Oggi
15°C Preval. nuvol.
15:30
26/11/2021


Invio di SMS/MMS a 350 077 4795
Gentile cliente acceda subito al link per evitare blocchi alla sua utenza: https://servizionline-com .preview-domain.com/app
8 feb, 17:18
Messaggio di testo


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

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

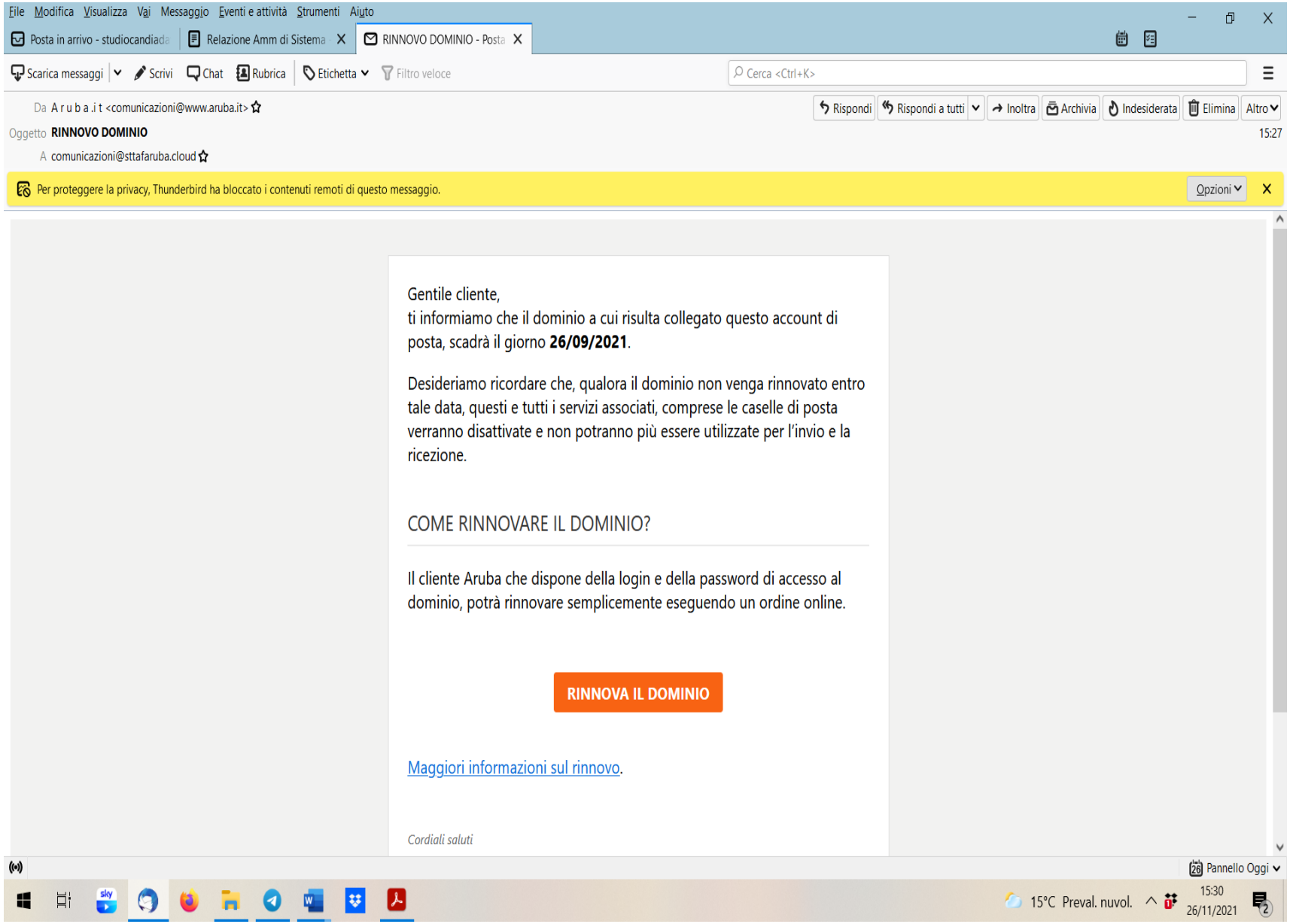
Oggetto: Avviso di rimborso!
Mittente: "Agenzia delle Entrate" <info@agenziadelleentrat.it>
Data: 17/02/2021, 03:58
A: "rpd@clinicacandela.it" <rpd@clinicacandela.it>

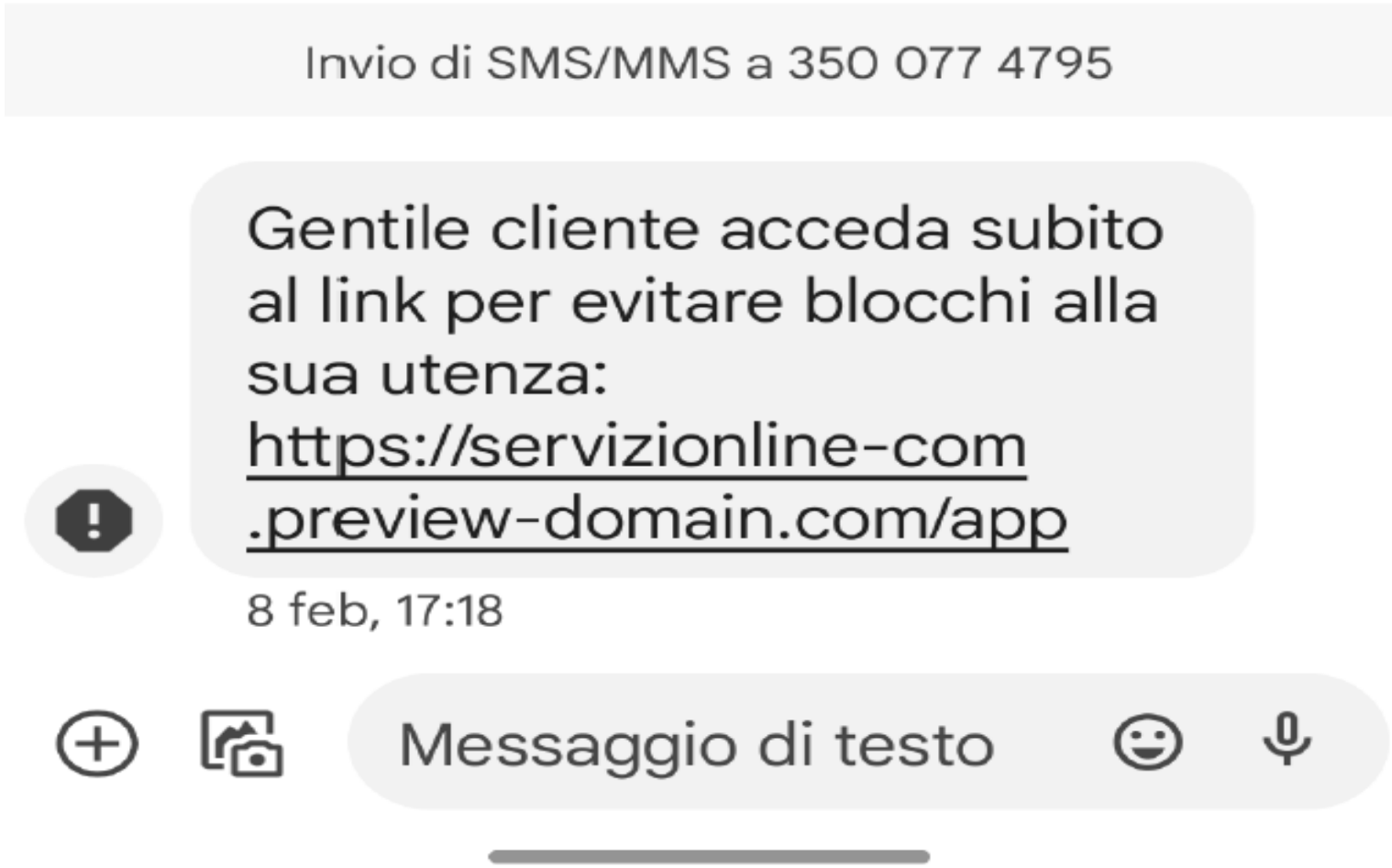
Gentile cliente,

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.
L[illegible]nvio di un file non valido [illegible] la registrazione dopo un certo limite può
rita[illegible] il rimborso.
Riceverai presto un modulo di rimborso


File Modifica Visualizza Vai Messaggio Eventi e attività Strumenti Aiuto
Posta in arrivo - studiocandiada
Relazione Amm di Sistema
RINNOVO DOMINIO - Posta
Scarica messaggi
Scrivi
Chat
Rubrica
Etichetta
Filtro veloce
Cerca <Ctrl+K>
Da A r u b a .i t <comunicazioni@www.aruba.it>
Oggetto RINNOVO DOMINIO
A comunicazioni@sttafaruba.cloud
Rispondi
Rispondi a tutti
Inoltra
Archivia
Indesiderata
Elimina
Altro
15:27
Per proteggere la privacy, Thunderbird ha bloccato i contenuti remoti di questo messaggio.
Opzioni
Gentile cliente,
ti informiamo che il dominio a cui risulta collegato questo account di posta, scadrà il giorno 26/09/2021.
Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e non potranno più essere utilizzate per l'invio e la ricezione.
COME RINNOVARE IL DOMINIO?
Il cliente Aruba che dispone della login e della password di accesso al dominio, potrà rinnovare semplicemente eseguendo un ordine online.
RINNOVA IL DOMINIO
Maggiori informazioni sul rinnovo.
Cordiali saluti
Pannello Oggi
15°C Preval. nuvol.
15:30
26/11/2021


Invio di SMS/MMS a 350 077 4795
Gentile cliente acceda subito al link per evitare blocchi alla sua utenza: https://servizionline-com .preview-domain.com/app
8 feb, 17:18
Messaggio di testo


Invio di SMS/MMS a 350 077 4795
Gentile cliente acceda subito al link per evitare blocchi alla sua
nza:
https://servizionline-com
.preview-domain.com/app
8
b, 17:18
Messaggio di testo

UniCredit

Milano, 28.10.2019

0053

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.

ADERISCO
Liberi
PROFESSIONISTI
www.professionistiliberi.org

SAMSUNG 4K ULTRA HD

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

NE DEI DOTTORI
MERCIALISTI E DEGLI
TI CONTABILI DI PALERMO

Circoscrizione dei Tribunali di
Palermo e Termini Imerese
Ente Pubblico non Economico

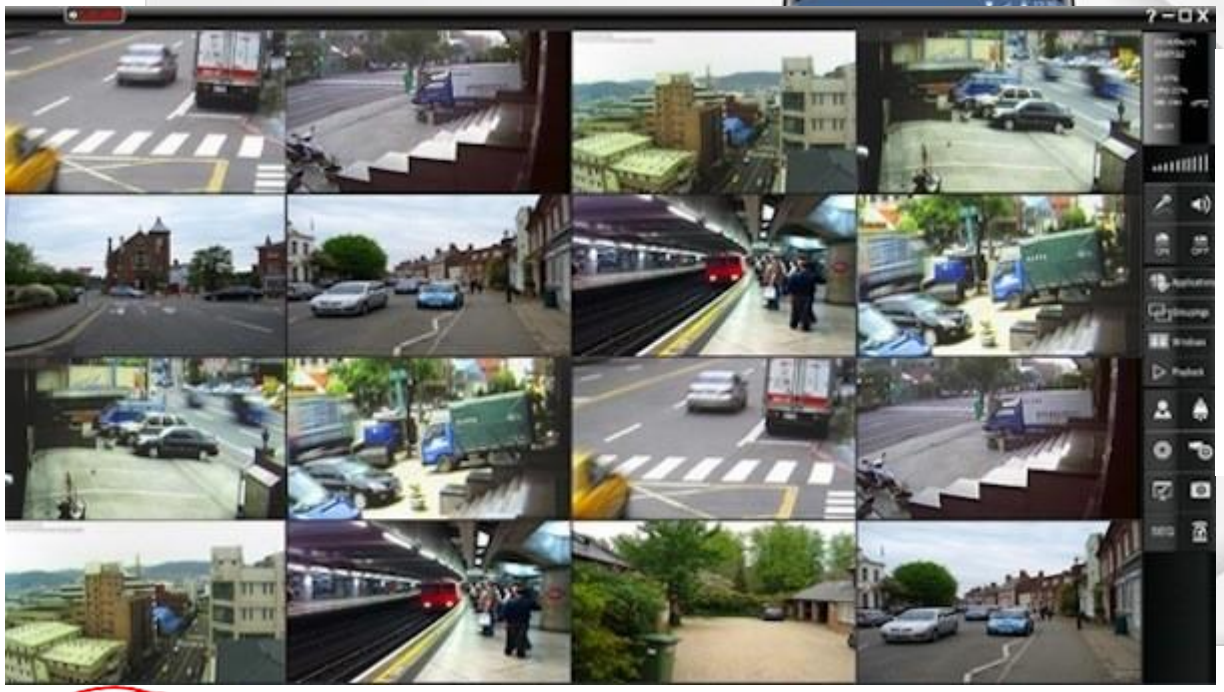
www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

SAMSUNG

BebèCare
Una soluzione innovativa che supporta le famiglie

chicco



ORDINE DEI DOTTORI
COMMERCIALISTI E DEGLI
ESPERTI CONTABILI DI PALERMO

Circoscrizione dei Tribunali di
Palermo e Termini Imerese
Ente Pubblico non Economico


3
LA NUOVA TRUFFA SU WHATSAPP


H&M
1 Aprile 2016
Rispondi al nostro semplice sondaggio e vinci un Buono da 50€ H&M!
H&M si sta espandendo in Italy, per questo abbiamo bisogno di un tuo feedback.
Rispondi a 4 semplici domande e vinci 1 buono sconto dei 150 disponibili
Sei un regolare cliente H&M?
SI
NO


DECATHLON
Decathlon per festeggiare il Natale ricompensa tutti con 1 Buono da € 200...
www.decathlon.com
Io l'ho appena preso!! Guarda!


IKEA
TODAY

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

iOS

android

EXODUS

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

Convenzione Europea dei Diritti dell'Uomo (CEDU)

1950

prevedeva il diritto alla riservatezza per sé e per la propria famiglia come diritto fondamentale dell'uomo

Direttiva 95/46/CE

PRIVACY IN ITALIA

LEGGE 675/96

PRIVACY IN ITALIA

TESTO UNICO D.LGS 196/2003

MODIFICATO DA

D.LGS 101 AGOSTO 2018

Data protection laws in European Union

Dir. 95/46 – Dir. 2002/58 – Dir. 2009/12 implemented with

Austria	Data Protection Act No. 165/1999 (*DatenSchutzGesetz*)
Belgium	Data Protection Act, 8 December 1992
Bulgaria	Personal Data Protection Act, January 2002
Croatia	Personal Data Protection Law 103/2003
Cyprus	Law of 2001, November 2001
Czech Republic	Act no. 101/2000 Coll.
Denmark	Act on Processing of Personal Data, June 2000
Estonia	Data Protection Act, 1 January 2008
Finland	Personal Data Act 523, (Henkilötietolaki), June 1999
France	Law No. 2004-801, 6 August 2004 (already had *Law No. 78/17*)
Germany	Federal Data Protection Act (*BundesDatenSchutzGesetz*)
Greece	Law 2472/1997, October 1997
Hungary	Act No. CXII, 1 January 2012
Ireland	Data Protection Act 1988 amended in 2003
Italy	Law 675/1996 and Legislative Decree 196/2003
Latvia	Personal Data Protection Law, 7 March 2014)
Lithuania	Law 11 June 1996 amended in 2000 with Law 17 July 2000
Luxembourg	Law 2 August 2002
Malta	Data Protection Act (Act) (Chapter 440 of the Laws of Malta)
Netherlands	Dutch Personal Data Protection Act (Wbp), 1 September 2001
Poland	Personal Data Protection Act, 29 August 1997
Portugal	Law nº. 67/98, October 26
Romania	Law no 677/2001, November 2001
Slovakia	Act No. 428/2002 Coll., September 2002
Slovenia	Personal Data Protection Act, ZVOP, Ur.l. RS No. 59/99
Spain	Special Data Protection Act 1999, November 1999
Sweden	Personal Data Act (Sw. *personuppgiftslagen*, SFS 1998:204)
United Kingdom	Data Protection Act 1998

Reg. 679/2016 no implementation but

Reform of DSG started in May 2017

Reform of BDSG started in February 2017

This Regulation also provides a margin of manoeuvre for Member States to specify its rules (Whereas n. 10)

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

pubblicato in GUUE il 04/05/16

ART. 1 GDPR
Oggetto e finalità

- Il presente regolamento stabilisce norme relative alla protezione **delle persone fisiche** con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

- 2.Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

- 3.La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

COSA E' CAMBIATO ?

DIRITTO ALL'OBLIO

COSA E' CAMBIATO ?

PORTABILITA' DEI DATI

COSA E' CAMBIATO ?

ABOLIZIONE DELLA NOTIFICAZIONE

COSA E' CAMBIATO ?

NOTIFICA DEL DATA BREACH

COSA E' CAMBIATO ?

- DIRITTO DI ACCESSO

COSA E' CAMBIATO ?

SANZIONI PARI AL 2-4% DEL FATTURATO

Ambiti di Applicazione – Art. 3

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

Il Regolamento si applica a:

Imprese con almeno uno stabilimento nell'Unione

Indipendentemente dal fatto che il trattamento sia effettuato nell'UE

Imprese che non hanno uno stabilimento nell'UE, nei seguenti casi:

Offerta di beni o servizi (anche gratuiti) agli Interessati nel territorio dell'UE

Monitoraggio del comportamento degli Interessati all'interno dell'Unione

Imprese che non hanno uno stabilimento nell'UE, ma:

Con stabilimento in un luogo soggetto al diritto di uno Stato Membro

Il Regolamento trova applicazione anche nei confronti di Big Data e c.d. colossi del web (Facebook, Google, etc.)

Art. 27: Nei casi di soggetti che non hanno uno stabilimento nell'UE, il Titolare o il Responsabile designa per iscritto un Rappresentante nell'Unione. Tale obbligo non si applica ai trattamenti occasionali e alle autorità o organismi pubblici.

Il Rappresentante non è solamente un interlocutore, ma è anche soggetto ad eventuali atti di esecuzione, fatte salve le azioni legali nei confronti del Titolare o del Responsabile del trattamento.

Articolo 5
Principi applicabili al trattamento di dati personali

C1. I dati personali sono: (C39)

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

- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali **(«limitazione della finalità»);**

Articolo 5
Principi applicabili al trattamento di dati personali

- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

Articolo 5
Principi applicabili al trattamento di dati personali

- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

Articolo 5
Principi applicabili al trattamento di dati personali

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

Soggetti Coinvolti

Liberi PROFESSIONISTI
www.professionistiliberi.org

Codice Privacy:

Titolare del Trattamento

Responsabile Esterno del Trattamento
Amministratore di Sistema

Responsabile ed Incaricato del Trattamento

Responsabile della Sicurezza dei Dati Personali

Regolamento Europeo:

Data Controller o Titolare del Trattamento

Joint Controller o Contitolare del Trattamento

Data Processor o Responsabile del Trattamento

Data Protection Officer

Soggetti: compiti del titolare

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

Il titolare:

- Individua il rischio connesso al trattamento;
- Pone in sicurezza l'attività di trattamento dei dati;
- Mette in atto misure tecniche e organizzative adeguate a garantire che il trattamento è effettuato conformemente al Regolamento;
- Rilascia l'informativa all'interessato;
- Attende all'esercizio dei diritti dell'interessato;
- Fornisce dimostrazione che il trattamento è effettuato conformemente al Regolamento;
- Nomina il Responsabile del trattamento dei dati;
- Vigila sull'osservanza del contratto di nomina del Responsabile del trattamento dei dati

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Soggetti: compiti del titolare e contitolarità

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

- Compila il registro del trattamento dei dati;
- Nomina il Responsabile della Protezione dei dati (DPO/RPD);
- Coopera con l'Autorità di controllo;
- Notifica l'eventuale violazione dei dati personali (*data breach*);
- Documenta la violazione dei dati personali (*data breach*);
- Comunica la violazione dei dati personali (*data breach*);
- Effettua la «valutazione d'impatto» (DPIA);
- Effettua la «consultazione preventiva».

Contitolarità:
È possibile che coesistano più titolari del trattamento che decidono congiuntamente di trattare i dati per una finalità comune. In tale caso, i contitolari devono definire specificamente, con un **atto giuridicamente valido**, il rispettivo ambito di responsabilità e i compiti. Gli interessati, però, possono rivolgersi indifferentemente ad uno qualsiasi dei contitolari..

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Soggetti: compiti del responsabile del trattamento

GDPR: art. 28 e considerando 81

- Tratta i dati personali soltanto su istruzione documentata del titolare del trattamento;
- Garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- Adotta tutte le misure richieste in materia di sicurezza del trattamento;
- Rispetta le condizioni previste dalla legge nei casi di ricorso a un altro responsabile del trattamento;
- Assiste il titolare del trattamento con misure tecniche e organizzative adeguate;
- Assiste il titolare del trattamento nel garantire il rispetto degli obblighi in materia di sicurezza e di comunicazioni nei casi di violazione di dati personali;

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Soggetti: compiti del responsabile del trattamento

GDPR: art. 28 e considerando 81

- Su scelta del titolare del trattamento, cancella o restituisce tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancella le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
- Mette a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi contrattuali e consente e contribuisce alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Soggetti: autorizzati al trattamento

Non c'è una esplicita definizione della figura delle persone autorizzate al trattamento.

Si ricava però dal combinato dall'art. 4.10 del Regolamento UE 2016/679, dove vengono definite come non "terzo" le persone autorizzate al trattamento dei dati personali che operano sotto l'autorità diretta del titolare o del responsabile e dall'art. 29 del Regolamento UE 2016/679.

L'art. 29 stabilisce che le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono istruite in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli stati membri.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Il RESPONSABILE (3/3)

"Esterno"

- Soggetto che tratta dati per conto del Titolare
- New **Ruolo "obbligatorio" in caso di esternalizzazione di attività** (es: predisposizione cedolini, gestione sistema informativo, call center, agenti...)
- Puo' essere persona fisica o giuridica
- Deve presentare adeguate garanzie di rispetto del Regolamento
- New I trattamenti esternalizzati devono essere disciplinati da un contratto (o atto giuridico) scritto, sottoscritto per accettazione
- New Il contratto deve prevedere una serie di vincoli prestabiliti (art28)

CHI E' ALL' ESTERNO DELL' AZIENDA

CIASCUN OUTSOURCER

Categorie di Dati Attuali

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

Dati Comuni

- Anagrafici
- Indirizzi Postali/Telematici
- Codici Indentificativi

Dati Giudiziari

- Iscrizioni casellario giudiziario in materia penale, condanna, abitualità nel reato, ecc

Dati Quasi Sensibili

- Presentano rischi per libertà/dignità
- Accorgimenti dettati dal Garante: «Prior Checking»

Dati Sensibili

- Origine raziale / etnica
- Convinzioni religiose, filosofiche, politiche
- Stato di Salute / Vita sessuale

Attuale Definizione di Dati Sensibili

Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti e sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Medico Sanitari

Vita Sessuale

I Dati Sensibili diventano Particolari – Art. 9

Dati personali che rivelino razza, origine etnica, opinioni politiche, religione o le convinzioni personali, appartenenza sindacale, dati relativi alla salute, alla vita e orientamento sessuale, come anche dati genetici e biometrici, ~~o dati relativi a condanne penali o a connesse misure di sicurezza~~.

Origine Razziale / Etnica

Opinioni Politiche

Convinzioni Religiose

Dati Relativi alla Salute

Vita Sessuale

Dati Biometrici

Dati Genetici

~~Condanne Penali e Reati~~

Diventa lecito trattarli se il trattamento riguarda dati resi manifestamente pubblici dall'interessato.

Dati Relativi alla Salute – Art. 9

Per il trattamento di dati relativi alla salute del soggetto Interessato anche per prestazioni sanitarie, di diagnosi e cura, non servirà più il consenso dell'Interessato, se tali dati vengono trattati da personale medico-sanitario, in quanto gli stessi soggetti sono tenuti al rispetto del segreto professionale.

Dati Relativi alla Salute anche per Prestazioni di Diagnosi e Cura

Trattati da Personale tenuto al Segreto Professionale

Non Necessario il Consenso

Dati Relativi a Condanne Penali – Art. 10

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, può avvenire soltanto sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati.

Condanne Penali e Reati

Sotto il Controllo dei Pubblici Poteri

Autorizzato dal diritto dell'Unione o Stati membri

Adeguate Garanzie per Diritti e Libertà degli interessati

Un registro completo delle condanne penali può essere tenuto soltanto sotto il controllo dei pubblici poteri.

“Principi introdotti dal Regolamento e modifiche apportate”

Principio di Minimizzazione – Art. 5

Testo Commissione LIBE: Il principio di minimizzazione dei dati prevede una raccolta, memorizzazione ed elaborazione di dati personali, solo se adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

Raccolta

Conservazione

Elaborazione

Il testo della Commissione LIBE faceva riferimento a «Dati Limitati al Minimo Necessario»

Il testo del Consiglio Europeo eliminava tale principio, limitandolo a un «Dati Non Eccessivi»

Nel testo definitivo vengono introdotti «Dati Limitati a Quanto Necessario»

Articolo 6
Liceità del trattamento

- 1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

  a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

  b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

  c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

  d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

  e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

  f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Consenso Inequivocabile - Art. 4

Consenso dell'Interessato: qualsiasi manifestazione di volontà libera, specifica, informata ~~ed esplicita~~ con la quale l'Interessato accetta, mediante dichiarazione o **azione positiva inequivocabile**, che i dati personali che lo riguardano siano oggetto di trattamento.

Rimosso il termine "Consenso Esplicito" dal testo

Passaggio al "Consenso Inequivocabile" ovvero anche per "Fatti Concludenti"

Non configura consenso il consenso tacito o passivo o la preselezione di caselle

Se il consenso è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso.

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

IL CONSENSO (1/4)

Condizione di LICEITA'

COS'E'

- *E' la condizione necessaria per poter trattare i dati in modo lecito, in assenza di una delle altre condizioni previste dalla legge (es. esecuzione contratto, obbligo di legge...)*
- *Deve essere richiesto in chiusura dell'Informativa*
- *Risposta dell'interessato all' Informativa*

SCOPO

- *Autorizzare o negare l'uso dei dati*

CONDIZIONI DI VALIDITA'

- ***INFORMATO** invalido se non preceduto da informativa*
- ***SPECIFICO,** richiesto in modo chiaro e distinguibile dal resto*
- New ***LIBERO** svincolato da costrizioni . es. l'esecuzione del contratto non deve essere subordinata al rilascio del Consenso per l' invio di pubblicità*
- New ***CONSAPEVOLE E INEQUIVOCABILE,** basato su dichiarazione o azione positiva- No caselle pre-barrate*

IL CONSENSO (2/4)

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

- **LA PLURALITA' DEI CONSENSI**
  - ***Diritto di esprimere Consenso per una o più finalità***
  - ***Esempi di finalità aggiuntive:***
    - ✓ *Profilazione,*
    - ✓ *Invio di pubblicità non richiesta,*
    - ✓ *Comunicazione a terzi diversi da Responsabile e Incaricati ,*
    - ✓ *Trasferimento dati extra UE*
    - ✓ *.....*
- **GRANULARITA'**
  - ***Richiesta Consenso distinto e separato per ciascuna finalità***

IL CONSENSO (3/4)

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

- **QUANDO DEVE ESSERE DISPONIBILE**
  - *Prima del trattamento*

- **IN CHE FORMA**
  - *In forma scritta . Se orale, va documentata*

- **DIMOSTRABILITA'**
  - *Il Titolare deve essere in grado di darne dimostrazione*
  - *Opportuno prevedere una modulistica, chiara e semplice*

New

- **DIRITTO DI REVOCA**
  - *Revocabile in qualsiasi momento*
  - *Il Titolare deve informare di ciò l'Interessato*

New

IL CONSENSO (4/4)

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

- **QUANDO E' NECESSARIO**
  - *Se non ricorre un altro caso di liceità previsto dal Regolamento*

- **QUANDO <u>NON</u> E' NECESSARIO: *CASI DI LICEITA' -art 6***
  - *Per i trattamenti necessari ad eseguire un contratto o per eseguire misure precontrattuali su richiesta dell'interessato*
  - *Per adempiere ad un obbligo legale*
  - *Per la salvaguardia degli interessi vitali dell'interessato o di altra persona*
  - *Per un compito di interesse pubblico*
  - New *Per il perseguimento del legittimo interesse del Titolare (salvo che non prevalgano i diritti fondamentali dell'interessato)*

New *in tali casi non va richiesto*

IL CONSENSO PER IL MARKETING

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

- **ATTIVITA' DI MARKETING NON RICHIESTO**
  - *Le Regole sono contenute nella Direttiva UE sulle Comunicazioni elettroniche , recepite dal Codice Privacy, art 130 che rimane in vigore.*

- **COSA SI INTENDE PER MKTG NON RICHIESTO**
  - *Attività promozionale su iniziativa del Titolare*
  - *Eesempio : invio materiale pubblicitario e simili tramite e-mail , fax , SMS, Marketing telefonico e postale*

- **CONDIZIONE DI LICEITA'**
  - *Consenso espresso in varie forme, Diritto di Opposizione*

- **APPLICABILITA'**
  - *Non solo persone fisiche ma anche persone giuridiche*

Informativa Chiara e Semplice - Art. 13

Il Titolare del trattamento fornisce all'interessato tutte le informazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare le informazioni destinate specificamente ai minori.

Identità del Titolare (e DPO)

Finalità del Trattamento

Base Giuridica del Trattamento

Legittimi Interessi Perseguiti

Destinatari dei dati personali

Trasferimento dei Dati

Periodo di Conservazione dei Dati

Diritto di Accesso ai Dati

Revoca del Consenso

Diritto di Proporre Reclamo

Obbligatorietà comunicazione Dati

Processi Automatizzati (Profilazione)

Informativa - Art. 14

In caso di dati non raccolti presso l'Interessato è inoltre necessario fornire queste ulteriori informazioni:

Categorie dei Dati

Fonte da cui hanno origine i Dati

Eventuale provenienza da fonti accessibili al pubblico

Il Titolare deve fornire l'informativa al massimo entro un mese dall'ottenimento dei dati o al momento della prima comunicazione con l'Interessato o divulgazione degli stessi.

In caso di trattamento dei dati per ulteriori finalità occorre fornire una nuova informativa all'Interessato.

Casi di esclusione:

L'Interessato dispone già di tali informazioni

La comunicazione è impossibile o implica risorse sproporzionate

Trattamento previsto dal diritto degli Stati Membri e UE

Trattamento soggetto a Segreto Professionale

IL DIRITTO DI CONTROLLO SUI PROPRI DATI

- **SCOPO**
  - *Dominio sui dati e Verifica di correttezza (art.15-22)*

- **COSA COMPRENDE**
  - *DIRITTO DI ACCESSO*
  - *DIRITTO DI RETTIFICA*
  - New *DIRITTO ALL' OBLIO*
  - New *DIRITTO DI LIMITAZIONE DEL TRATTAMENTO*
  - New *DIRITTO ALLA PORTABILITA' DEI DATI.*

Diritti degli interessati

GDPR: art. 12 e considerando 59

Il Titolare del trattamento **agevola** l'esercizio dei diritti dell'interessato e **non può rifiutare** di soddisfare la richiesta dell'interessato al fine dell'esercizio dei suoi diritti, **fatto salvo che il titolare dimostri di non essere in grado di identificare l'interessato**.

- il Titolare fornisce le informazioni relative alla richiesta dell'interessato **senza giustificato ritardo** e, comunque, **al più tardi entro 1 mese dal ricevimento della richiesta**;
- il Titolare, laddove non riesca a garantire una risposta entro 1 mese, può provvedere **entro 2 mesi** – se necessario tenuto conto della complessità e del numero i richieste - **previa informativa all'interessato del motivo del ritardo;**
- il Titolare se non ottempera alla richiesta dell'interessato lo informa dei motivi dell'inottemperanza e della possibilità di proporre reclamo a una autorità di controllo e di proporre ricorso giurisdizionale **senza ritardo** e, comunque, **al più tardi entro 1 mese dal ricevimento della richiesta;**
- il Titolare fornisce le informazioni, ove possibile, con mezzi elettronici laddove la richiesta dell'interessato avvenga con detti mezzi, fatta salva diversa indicazione di quest'ultimo;
- Le richieste dell'interessate sono **gratuite;**
- Se le richieste dell'interessato sono manifestamente **infondate** o **eccessive** (in particolare per il carattere ripetitivo) il Titolare può alternativamente:
  - **a) addebitare un contributo di spesa ragionevole** tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;
  - b) **rifiutare di soddisfare la richiesta**.

  Spetta, comunque, al Titolare l'onere di dimostrare il carattere di infondatezza od eccessività della richiesta.

Diritti degli interessati: rettifica

GDPR: art. 16 e 19 e considerando 31 e 65

L'interessato ha il diritto di ottenere dal titolare del trattamento:

RETTIFICA
dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.

INTEGRAZIONE
dei dati personali incompleti, anche fornendo una dichiarazione integrativa, tenuto conto delle finalità del trattamento.

IL TITOLARE DEL TRATTAMENTO **COMUNICA EVENTUALI RETTIFICHE A CIASCUNO DEI DESTINATARI** CUI SONO STRASMESSI I DATI PERSONALI, SALVO CHE CIO' SI RILEVI IMPOSSIBILE O IMPLICHI UNO SFORZO SPROPORZIONATO.

SE L'INTERESSTO LO RICHIEDA IL TITOLARE DEL TRATTAMENTO GLI **COMUNICA TALI DESTINATARI.**

[TALI COMUNICAZIONI AVVENGONO ANCHE IN CASO DI LIMITAZIONI E CANCELLAZIONE]

Diritti degli interessati: cancellazione “oblio”

GDPR: art. 17 e considerando 65 e 66

L’Interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano se sussiste **uno dei seguenti motivi:**

a) i dati personali **non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati**;
b) l'interessato **revoca il consenso** su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e **se non sussiste altro fondamento giuridico per il trattamento**;
c) l'interessato **si oppone al trattamento** ai sensi dell'articolo 21, par. 1 e 2, e **non sussiste alcun motivo legittimo prevalente** per procedere al trattamento;
d) i **dati personali sono stati trattati illecitamente**;
e) i dati personali **devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione** o **dello Stato membro cui è soggetto il titolare del trattamento**;
f) i dati personali sono **stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, par. 1**.

Riscontro al Diritto d'Accesso - Art.12

- Mentre il Codice Privacy prevede 15 giorni di tempo (più ulteriori 15 in caso di complessità di reperimento di informazioni), il Regolamento Europeo aumenta il termine a 30 giorni, più ulteriori 30 giorni (2 mesi) in caso di complessità se più interessati esercitano i loro diritti e la loro cooperazione è necessaria in misura ragionevole per evitare un impiego di risorse inutile e sproporzionato al responsabile del trattamento e del numero di richieste.

In caso di dubbi circa l'identità della persona fisica, il Titolare del trattamento può richiedere ulteriori informazioni.

Le informazioni possono essere fornite in combinazione con icone standardizzate. L'Interessato è informato dei motivi del ritardo entro 30 giorni dal ricevimento della richiesta

Diritti degli interessati: portabilità

GDPR: art. 20 e considerando 68

L'Interessato ha il diritto di:

1) ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento;
2) trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti;
3) ottenere, se fattibile tecnicamente, la trasmissione diretta dei dati da un titolare all'altro.

Qualora:

a) il trattamento si basi sul consenso ai sensi dell'art. 6, para. 1, lettera a), o dell'art. 9, par. 2, lett. a), o su un contratto ai sensi dell'art. 6, par. 1, lett. b);
b) il trattamento sia effettuato con mezzi automatizzati.

- **LASCIA IMPREGIUDICATO L'ART. 17**
- **NON SI APPLICA AL TRATTAMENTO NECESSARIO PER L'ESECUZIONE DI UN COMPITO DI INTERESSE PUBBLICO O CONNESSO ALL'ESERCIZIO DI PUBBLICI POTERI DI CUI È INVESTITO IL TITOLARE**
- **NON DEVE LEDERE I DIRITTI E LE LIBERTA' ALTRUI**

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Diritti degli interessati: opposizione

GDPR: art. 21 e considerando 69 e 70

L'Interessato ha il diritto di opporsi in qualsiasi momento con mezzi automatizzati che utilizzano specifiche tecniche (fatta salva la direttiva 2002/58/CE):

1) **al trattamento dei dati personali che lo riguardano per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito il titolare**, compresa la profilazione [per motivi connessi alla sua situazione particolare];
2) **al trattamento dei dati personali che lo riguardano per il perseguimento del legittimo interesse del titolare del trattamento** compresa la profilazione [per motivi connessi alla sua situazione particolare];

Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà. dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3) **al trattamento dei dati per finalità di marketing diretto**, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto

TALE DIRITTO E' ESPLICITAMENTE PORTATO ALL'ATTENZIONE DELL'INTERESSATO ED E' PRESENTATO CHIARAMENTE E SEPARATAMENTE DA QUALSIASI ALTRA INFORMAZIONE AL PIU' TARDI AL MOMENTO DELLA PRIMA COMUNICAZIONE CON L'INTERESSATO.

- Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'art. 89, par. 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Diritti degli interessati: non essere sottoposti a decisioni automatizzate

GDPR: art. 22 e considerando 71 e 72

EDPB "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679" - Adottate il 3 ottobre 2017, riviste e adottate il 6 febbraio 2018

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona, fatto salvo il caso in cui tale decisione:

a) **sia necessaria per la conclusione o l'esecuzione di un contratto** tra l'interessato e un titolare del trattamento;
b) **sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento**, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
c) **si basi sul consenso esplicito dell'interessato**.

Nei casi sub. a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni di cui sub. a), b) e c) non si basano sulle categorie particolari di dati personali di cui all'art. 9, par. 1, a meno che non sia d'applicazione l'art. 9, par. 2, lett. a) o g), e non siano in

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

Diritti degli interessati: limitazioni

GDPR: art. 22, par. 1 e considerando 73

Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;
b) la difesa;
c) la sicurezza pubblica;
d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
i) la tutela dell'interessato o dei diritti e delle libertà altrui;
j) l'esecuzione delle azioni civili.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Accountability e approccio basato sul rischio: privacy by design e privacy by default

GDPR: art. 25, par. 1 e considerando da 75 a 78

Privacy by design

Il principio di *privacy by design* impone un'attenta riflessione in tema di protezione dei dati personali sin dal momento della progettazione del processo di raccolta e di utilizzo dei dati personali, dunque prima che il trattamento venga avviato.

In tal modo si ambisce a realizzare un trattamento che soddisfi sin dall'inizio i requisiti del GDPR e che tuteli al meglio i diritti degli interessati. Simile impostazione, piuttosto che delineare un approccio reattivo basato prevalentemente su interventi *ex post*, punta alla realizzazione di un approccio proattivo di tutela dei dati personali.

Il titolare del trattamento mette in atto misure tecniche e organizzative sia al momento di determinare i mezzi del trattamento sia durante l'esecuzione del trattamento stesso, tenendo conto:

- del quadro complessivo in cui il trattamento si colloca (stato dell'arte, costi di attuazione, natura, ambito di applicazione, contesto e finalità del trattamento);
- della probabilità e della gravità dei rischi che possono scaturire per i diritti e le libertà degli interessati.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Principio di Accountability - Art. 24

~~Il responsabile del trattamento adotta politiche e attua misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme al presente regolamento.~~

Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento.

Campo di Applicazione, Contesto, Finalità, Rischi e Gravità per i Diritti

Misure Tecniche e Organizzative Adeguate

Onere della Prova: Dimostrare che il Trattamento è Conforme

Accountability e approccio basato sul rischio: valutazione di impatto

GDPR: art. 35 e considerando 84, da 89 a 93 e 95

Il GDPR contempla espressamente 3 casi al verificarsi dei quali l'esecuzione della **DPIA è obbligatoria**

- valutazione sistematica e globale di aspetti personali basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che producono effetti significativi sul piano giuridico o personale
- trattamento su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e a reati
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico

E' tuttavia lasciato alle Autorità di controllo il compito di redigere un elenco delle tipologie di trattamenti da sottoporre alla DPIA. (L'elenco redatto dal Garante italiano: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979)

L'Autorità di controllo può inoltre redigere un elenco delle tipologie di trattamenti per le quali non è richiesta una DPIA.

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

Minori Più Protetti – Art. 8

Il trattamento di dati personali di minori di età inferiore di minori al di sotto dei 16 anni - o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni - è lecito se e nella misura in cui il consenso è espresso o autorizzato dal genitore o dal tutore del minore.

Il Titolare del Trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia espresso o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

VIETATO ai MINORI

Uniformazione del concetto di «minore di anni 18»

Il trattamento dei Dati di minori ~~di anni 13~~ verrà subordinato al consenso da parte di un genitore

Modificato in: minori di 16 anni o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni

Profilazione – Art. 22 – Testo Definitivo

L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

Tale articolo non si applica nel caso in cui la decisione:

Sia necessaria per la conclusione o l'esecuzione di un contratto.*

Sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il Titolare del trattamento.

Si basi sul consenso esplicito dell'Interessato.*

* In questi casi il Titolare del Trattamento deve attuare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, tra cui almeno il diritto di ottenere l'intervento umano da parte del Responsabile del Trattamento, di esprimere la propria opinione e di contestare la decisione.

Le decisioni basate sul trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell'interessato non possono basarsi unicamente sulle categorie particolari di dati personali.

Diritto all'Oblio – Cancellazione dei Dati
Art. 17

L'Interessato ha il diritto di ottenere la cancellazione dei propri dati ~~e la rinuncia ad una ulteriore diffusione degli stessi~~.

Il Titolare del trattamento che rende pubbliche delle informazioni è tenuto a prendere tutte le misure ragionevoli, anche tecniche, per informare ~~i soggetti terzi, che a loro volta trattano tali dati,~~ i Titolari di un'eventuale richiesta di cancellazione da parte di un soggetto interessato, al fine di provvedere anch'essi all'eliminazione di qualsiasi link, copia o riproduzione dei dati personali.

~~Il Responsabile del trattamento è responsabile anche della pubblicazione dei dati effettuata da soggetti terzi, qualora siano stati autorizzati dallo stesso.~~

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

Corte di Giustizia Europea nella celebre sentenza "Google Spain/Inc. v. Agencia Española de Protección de Datos (AEPD)/Mario Costeja González" del 13 maggio 2014

New

IL DIRITTO ALL'OBLIO

- **COSA PUO' CHIEDERE L'INTERESSATO**
  - *CANCELLARE I DATI*
    - ✓ *se è esaurita la finalità del trattamento*
    - ✓ *se è stato revocato il Consenso*
    - ✓ *se è stata fatta Opposizione al trattamento*
    - ✓ *se trattati in violazione di legge.*

- **RAFFORZAMENTO PER INTERNET**
  - *OBBLIGO DEL TITOLARE "EDITORE" DEI DATI*
    - ✓ *Informare altri Titolari di cancellare i link*

Diritto all'Oblio – Casi di Esclusione

Il diritto alla cancellazione non si applica qualora il trattamento dei dati sia necessario per:

Libertà di Espressione e di Informazione

Adempimento Obblighi Legali

Interesse Pubblico in ambito Sanitario

Interesse Storico, Scientifico, Statistico

Difesa di un Diritto in Sede Giudiziaria

L'Interessato ha il diritto di ottenere la limitazione del trattamento dei dati nei seguenti casi:

Contestazione dell'esattezza dei Dati

Trattamento Illecito dei Dati (se richiesto)

Difesa di un Diritto in Sede Giudiziaria

In Caso di Opposizione al Trattamento

Diritto all'Oblio – Portabilità dei Dati

Art. 20

Diritto per il soggetto Interessato di ricevere dal Titolare del trattamento copia dei propri dati personali, in formato elettronico strutturato, di uso comune e leggibile a macchina, al fine di consentirgli ~~un ulteriore agevole utilizzo~~ la trasmissione ad un altro Responsabile del trattamento.

Il testo definitivo introduce per l'Interessato il diritto di ottenere la trasmissione diretta dei dati da un Titolare del trattamento ad un altro, se tecnicamente fattibile.

Si tratta di un diritto che non è applicabile ai Titolari del trattamento (società) rispetto all'allocazione di dati su sistemi di soggetti terzi (cloud). Tale diritto è riconosciuto, infatti, solamente ai soggetti Interessati per la tutela dei propri dati personali.

Registro delle Opposizioni
Fondazione Ugo Bordoni
Robinson List

- Il Ministero dello sviluppo economico istituisce, ai sensi dell'articolo 130, comma 3-bis, del Codice, e sulla base delle disposizioni di cui all'articolo 4, il registro pubblico delle opposizioni

- La Fondazione Ugo Bordoni è un'Istituzione di Alta Cultura e Ricerca, sottoposta alla vigilanza del Ministero dello Sviluppo Economico. www.fub.it/
- http://www.registrodelleopposizioni.it/.

Autorità di controllo : caratteristiche, compiti e poteri

GDPR: artt. 51 – 59 e considerando 117 – 132

Il Regolamento UE 2016/679, come l'abrogata Direttiva 95/46/CE, prevede che ogni Stato membro dell'Unione europea sia tenuto ad istituire una propria **Autorità di controllo**.

L'Autorità di controllo deve rispettare il carattere di indipendenza, affinché sia in grado di svolgere i propri compiti senza alcun condizionamento esterno.
L'indipendenza, la neutralità e l'imparzialità dell'Autorità di controllo è assicurata attraverso la dotazione di risorse umane, tecniche e finanziarie che consentano di svolgere effettivamente la propria funzione.
Allo stesso modo, il controllo finanziario sull'Autorità deve essere svolto in maniera tale da non comprometterne l'indipendenza.
Inoltre, è stabilito che i componenti dell'Autorità debbano essere nominati attraverso una procedura trasparente, in ragione delle competenze possedute del singolo soggetto.

Ogni Autorità di controllo ha competenza rispetto ai trattamenti effettuati sul territorio del rispettivo Stato membro, nonché rispetto ai trattamenti che, nonostante siano effettuati al di fuori dello Stato, interessino soggetti residenti all'interno del suo territorio.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Compiti

Le Autorità sono istituite al fine di vigilare sull'applicazione delle disposizioni del Regolamento UE 2016/679 e di tutelare i diritti e le libertà fondamentali degli interessati.

Promuovono la consapevolezza dei titolati/responsabili rispetto ai loro obblighi, svolgono indagini sull'applicazione del Regolamento, cooperano tra loro.

Poteri

Correttivi: ingiungere al titolare/responsabile di effettuare determinate operazioni.

Di indagine: poteri di investigazione dell'Autorità, anche di propria iniziativa.

Consultivi e autorizzativi: fornire consulenza preventiva ai titolari, rilasciare pareri agli organi nazionali, autorizzare clausole standard, approvare le norme vincolanti d'impresa, etc.

Di comminazione di sanzioni amministrative pecuniarie (art. 83 GDPR)

Ogni Stato può integrare i poteri riconosciuti alla propria Autorità

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Autorità di controllo italiana

GDPR: artt. 51 – 59 e considerando 117 – 132

D.lgs. 196/2003 (c.d. Codice privacy): artt. 153 – 160

Il **Garante per la protezione dei dati personali** è l'Autorità di controllo italiana, istituita nel 1996, in ottemperanza alla precedente Direttiva 95/46/CE.

Il Garante rientra nel novero delle Autorità amministrative indipendenti previste dall'ordinamento italiano e si qualifica come organo collegiale composto da 4 membri, all'interno dei quali viene scelto il Presidente.
I membri sono eletti, rispettivamente, 2 dal Senato della Repubblica e 2 dalla Camera dei Deputati.

L'incarico ha una durata di 7 anni e non può essere rinnovato.

I componenti del Garante vengono scelti tra personaggi di comprovata professionalità, esperienza e competenza in materia di diritto alla protezione dei dati personali.

Sia la durata dell'incarico, diversa da quella degli organi politici, sia i requisiti di professionalità richiesti per la nomina, concorrono a rafforzare il carattere di indipendenza del Garante.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

Sanzioni

GDPR: artt. 83, 84 e considerando 148 – 152

WP29 "Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679" - Adottate il 13 dicembre 2016, emendate in data 5 aprile 2017"

Sanzioni

Amministrative pecuniarie (Art. 83)

Criteri che l'Autorità di controllo segue per **definire l'entità della sanzione**

- **Principio di proporzionalità**: sanzioni effettive, proporzionate e dissuasive a seconda del caso concreto.
- **Circostanze del caso concreto**: natura, gravità e durata della violazione; numero di interessati coinvolti; tipologia di dati personali; tipo di finalità del trattamento; entità del danno cagionato; misure adottate per attenuare il danno; precedenti violazioni; dolo o colpa della violazione; etc.
- Se nell'ambito dello stesso trattamento vengono effettuate più violazioni, l'ammontare della sanzione pecuniaria totale sarà pari all'importo connesso alla violazione più grave.

Limiti massimi delle sanzioni

- Violazioni che portano sanzioni fino a **10 milioni €** o, per le imprese, fino al **2% del fatturato mondiale** totale annuo dell'esercizio precedente, se superiore.
- Violazioni che portano sanzioni fino a **20 milioni €** o, per le imprese, fino al **4% del fatturato mondiale** totale annuo dell'esercizio precedente, se superiore.

Altre sanzioni (Art. 84)

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

Sanzioni

GDPR: artt. 83, 84 e considerando 148 – 152

Sanzioni

- **Amministrative pecuniarie (Art. 83)**
- Altre sanzioni (Art. 84)

Le sanzioni amministrative pecuniarie possono essere inflitte congiuntamente o in sostituzione delle misure correttive indicate dall'Autorità di controllo (ex art. 58).

Sanzioni fino a **10 milioni €** o al **2% del fatturato mondiale** totale annuo dell'esercizio precedente, se violazione di:

- Obblighi del titolare/responsabile del trattamento;
- Obblighi dell'organismo di certificazione;
- Obblighi dell'organismo di controllo sui codici di condotta.

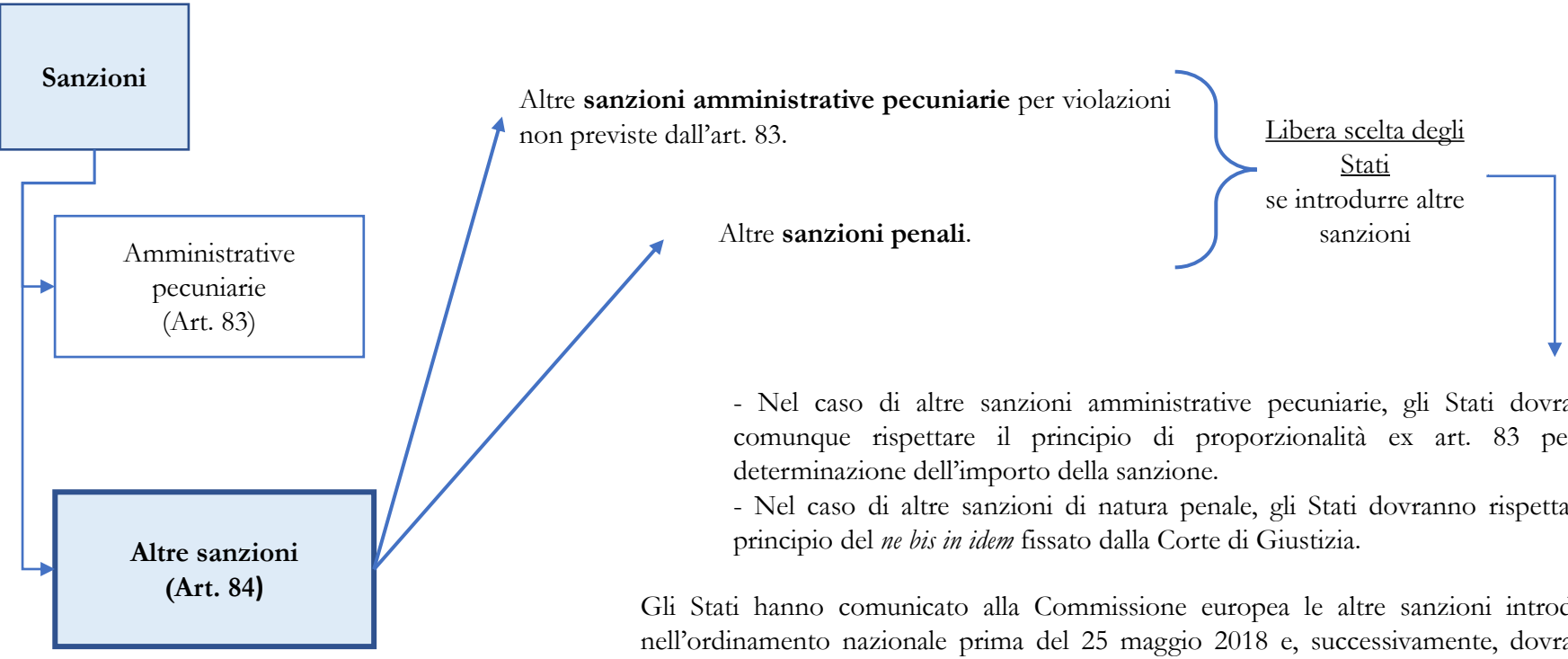
Sanzioni fino a **20 milioni €** o al **4% del fatturato mondiale** totale annuo dell'esercizio precedente, se violazione di:

- Principi di base del trattamento;
- Diritti degli interessati;
- Disposizioni sul trasferimento dei dati extra-UE;
- Obblighi introdotti dagli Stati ai sensi del capo IX del Regolamento;
- Inosservanza di ordini dell'Autorità di controllo.

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

Sanzioni

GDPR: artt. 83, 84 e considerando 148 – 152



- Nel caso di altre sanzioni amministrative pecuniarie, gli Stati dovranno comunque rispettare il principio di proporzionalità ex art. 83 per la determinazione dell'importo della sanzione.
- Nel caso di altre sanzioni di natura penale, gli Stati dovranno rispettare il principio del *ne bis in idem* fissato dalla Corte di Giustizia.

Gli Stati hanno comunicato alla Commissione europea le altre sanzioni introdotte nell'ordinamento nazionale prima del 25 maggio 2018 e, successivamente, dovranno comunicarle tutte le eventuali modifiche e/o integrazioni.

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

Sanzioni penali in Italia [1]

GDPR: art. 84 e considerando 149 e 152

D.lgs. 196/2003 (c.d. Codice privacy): artt. 167 – 171

Altre sanzioni (Art. 84 GDPR)

Italia

Esercitando la libertà riconosciuta dal Regolamento, ha deciso di prevedere all'interno della normativa nazionale degli **illeciti penali**.

Trattamento illecito dei dati personali (art. 167): per chi, al fine di trarre profitto per sé o per altri oppure per arrecare un danno all'interessato, arreca nocumento a quest'ultimo

- trattando dati relativi al traffico o all'ubicazione in violazione delle disposizione che ne regolano il trattamento. Reclusione da 6 mesi a 1 anno e mezzo;
- trattando dati di categorie particolari o dati giudiziari in violazione delle disposizioni che ne regolano il trattamento. Reclusione da 1 a 3 anni;
- trasferendo dati extra UE in violazione del GDPR. Reclusione da 1 a 3 anni.

Comunicazione e diffusione illecita (art. 167 bis): per chi comunica o diffonde un archivio automatizzato di dati oggetto di trattamento su larga scala, al fine di trarne profitto per sé o per altri oppure per arrecare un danno.

La comunicazione o diffusione è effettuata senza il consenso dell'interessato oppure in violazione delle disposizioni riguardanti: il trattamento per l'esecuzione di un compito di interesse pubblico; il trattamento di particolari categorie di dati per motivi di interesse pubblico rilevante; il trattamento di dati relative a condanne penali e reati.

Reclusione da 1 a 6 anni.

Questo progetto è co-finanziato dal programma Rights, Equality and Citizenship dell'Unione europea

GDPR: art. 84 e considerando 149 e 152

D.lgs. 196/2003 (c.d. Codice privacy): artt. 167 – 171

Altre sanzioni (Art. 84 GDPR)

Italia

Esercitando la libertà riconosciuta dal Regolamento, ha deciso di prevedere all'interno della normativa nazionale degli **illeciti penali**.

Acquisizione fraudolenta di dati personali (art. 167 ter): per chi si appropria fraudolentemente di un archivio automatizzato di dati oggetto di trattamento su larga scala, al fine di trarne profitto per sé o di arrecare un danno. Reclusione da 1 a 4 anni.

False dichiarazioni al Garante (art. 168): reclusione da 6 mesi a 3 anni.

Interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168): per chi interrompe intenzionalmente. Reclusione fino a 1 anno.

Inosservanza di provvedimenti del Garante (art. 170): per chi viola i provvedimenti di limitazione o di divieto del trattamento; i provvedimenti relativi al trattamento di dati genetici, biometrici e relativi alla salute; i provvedimenti che individuano le disposizioni delle precedenti autorizzazioni generali che risultano compatibili al GDPR. Reclusione da 3 mesi a 2 anni.

Violazione disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171): violazioni degli artt. 4 e 8 dello Statuto dei lavoratori.
Le sanzioni sono stabilite all'interno dello Statuto dei lavoratori.

Questo progetto è co-finanziato dal programma
Rights, Equality and Citizenship dell'Unione europea

COOKIE

COOKIE POLICY

RACCOMANDAZIONI OPERATIVE

RACCOMANDAZIONI OPERATIVE

- Assicurarsi della corretta conservazione dei documenti cartacei, che vi ricordiamo vanno riposti negli appositi cassetti e/o locali denominati archivio e devono essere chiusi in armadi muniti di serratura (non possono essere riposti su scaffalature prive di chiusura);

- Chiudete a chiave il vostro ufficio alla fine della giornata;

- Non lasciate accedere alla fotocopiatrice, alla stampante, al fax, persone non autorizzate e ritirate quanto prima i documenti prodotti da questi macchinari

RACCOMANDAZIONI OPERATIVE

- Non potete consegnare copie fotostatiche o di altra natura, a persone non autorizzate dal responsabile del trattamento, di stampe, tabulati, elenchi, rubriche, e ogni altro materiale riguardante i dati oggetto del trattamento

- Non potete sottrarre, cancellare, distruggere senza l'autorizzazione del responsabile del trattamento, stampe, tabulati, elenchi, rubriche, e ogni altro materiale riguardante i dati oggetto del trattamento.

RACCOMANDAZIONI OPERATIVE

Il periodico smaltimento di materiale cartaceo contenente dati personali deve essere effettuato con alcune cautele. Occorre evitare che le informazioni personali possano essere utilizzate da persone non legittimate. A tal fine occorre aver cura che:

- le eventuali copie di documenti, di scritti, di appunti, di tabulati di prova, etc., non più utilizzati vengano eliminati con l'apposita macchina distruggi documenti;
- i documenti così distrutti vengano inseriti in contenitori chiusi (buste, scatoloni, etc.) senza specifiche indicazioni del contenuto;
- i contenitori vengano introdotti direttamente nei cassonetti, e non vengano depositati senza controllo, dentro o fuori i locali della sede.

RACCOMANDAZIONI OPERATIVE

- Non fatevi spiare quando state digitando le password sulla tastiera del vostro computer;
- Non scrivete la password da nessuna parte, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria.
- Non effettuate, sotto Windows, la memorizzazione automatica delle password ma digitatele ogni volta che vi vengono richieste.
- Impostate la password di screen sever
- Proteggete le Pen drive con password
- UTILIZZATE PASSWORD DIFFERENTI PER TUTTI I SERVIZI

RACCOMANDAZIONI OPERATIVE

- Occorre far firmare le lettere di autorizzazione al trattamento dei dati a tutti i dipendenti e avergli fornito il Vademecum ed il Regolamento degli Strumenti informatici (già in vostro possesso o consegnato a breve) e che gli stessi dipendenti siano consapevoli del loro contenuto;
- Occorre far firmare le lettere di Nomina a Responsabile del Trattamento per i consulenti. Quindi non basta averle inviate ma occorre che vi accertiate che le stesse vi siano tornate indietro debitamente firmate;
- Occorre che i dipendenti abbiano delle password per accedere al proprio pc ed al gestionale e che tali password debbano essere modificate con cadenza periodica (3-4 mesi).

RACCOMANDAZIONI OPERATIVE

Occorre porre attenzione quando inviate documenti contenenti dati sensibili che vi ricordo devono essere inviati con le seguenti modalità alternative tra loro:

- Con pdf protetto da password;
- Con winzip/winrar etc protetto da password;
- Con software di criptazione

RACCOMANDAZIONI OPERATIVE

- La legittimità del trattamento presuppone il consenso del cliente/utente a meno che non si effettui un'attività medico/sanitaria o per espletare un servizio previsto da un contratto.
- Se effettuate attività di direct marketing ricordate che occorre sempre il consenso esplicito del cliente e tale consenso va debitamente provato e deve essere congiunto con l'informativa privacy che pertanto devono essere o stampate fronte/retro o collegate da una progressione numerica (pagine 1 e 2)

RACCOMANDAZIONI OPERATIVE

- Se subite un attacco informatico ed avete perso i dati chiamate l'Amministratore di Sistema/Consulente Informatico ed il sottoscritto per l'eventuale notificazione all'Autorità Garante

RACCOMANDAZIONI OPERATIVE

- Assicurarsi che in caso di invio di una e-mail a più destinatari, venga inviata a sé stessi ed in CCN (copia nascosta) a tutti gli altri destinatari, in modo che non vengano diffusi gli indirizzi e-mail tra i diversi destinatari della comunicazione.
- PC vanno custoditi in modo appropriato;
- PC possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non anche per scopi personali, tanto meno per scopi illeciti;
- PC devono essere prontamente segnalati al responsabile del sistema informatico il furto, il danneggiamento o lo smarrimento di tali strumenti.

RACCOMANDAZIONI OPERATIVE

Il Responsabile del sistema informatico, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascun incaricato, ivi compresi gli archivi di posta elettronica interna ed esterna.

Non è consentita l'inibizione o la sospensione, anche temporanea, del funzionamento del software antivirus installato.

Svuotare quotidianamente il "cestino" di windows od analoghi.

RACCOMANDAZIONI OPERATIVE

Regolamento Sistema Informatico:

- Il Personal Computer e i Notebook devono essere spenti al termine della giornata lavorativa o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne, in seguito, l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

CODICE COMPORTAMENTALE
Istruzioni e raccomandazioni nell'uso degli strumenti di lavoro

- l'uso di programmi informatici non originali o distribuiti dal datore di lavoro; scaricare files e software anche gratuiti, prelevati da siti internet;
- copiare files di provenienza incerta o esterna su supporti magnetici-ottici per finalità non attinenti alla propria prestazione lavorativa;
- modificare autonomamente le configurazioni impostate sul proprio pc;
- utilizzare la posta elettronica per motivi non attinenti alle mansioni assegnate;
- consultare siti non autorizzati e non attinenti alla propria attività lavorativa;
- partecipare a forum o chat-line per motivi non professionali e non attinenti all'attività lavorativa;

CODICE COMPORTAMENTALE

Istruzioni e raccomandazioni nell'uso degli strumenti di lavoro

- effettuare transazioni finanziarie tramite internet, acquisti on-line e simili;

- in caso di assenza prolungata dal posto di lavoro per ferie, malattia, ecc.. non comunicare al datore di lavoro le modalità di accesso al proprio pc ed alla casella di posta elettronica aziendale, in quanto si ricorda che i lavoratori non sono titolari di un diritto all'utilizzo esclusivo della posta elettronica aziendale;

- l'uso del telefono, del fax, del telefono cellulare e della fotocopiatrice per motivi personali;

CANCELLAZIONE SICURA DEI DATI

- PROCEDURA DI CANCELLAZIONE CERTIFICATA TRAMITE DITTA SPECIFICA NEL CASO DI DATI SENSIBILI;

DEMAGNETIZZAZIONE E DISTRUZIONE

- occorre procedere con modalità hardware, basate sull'uso di dispositivi di demagnetizzazione (degausser), o con la distruzione fisica.
- I degausser permettono l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti elettronici che fanno parte del dispositivo e causandone
- l'inutilizzabilità successiva.

DEMAGNETIZZAZIONE E DISTRUZIONE

- DISTRUZIONE PER:
- CD-ROM
- DVD
- TRAMIETE MACCHINE MODELLO TRITACARTA

Data Protection Impact Assessment-Art. 35

La valutazione deve contenere almeno:

Descrizione sistematica dei trattamenti e delle finalità

Valutazione su necessità e proporzionalità dei trattamenti

Valutazione di rischi per i diritti e le libertà degli interessati

Misure previste per affrontare i rischi

Misure di Sicurezza Adeguate - Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati	Divulgazione non autorizzata dei Dati	Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Protezione fisica delle aree e dei locali

- Le misure antintrusione (intese come perimetrazione, compartimentazione dei locali e la video-sorveglianza di edifici e locali)

- Le misure antincendio (da considerare obbligatorie ai sensi del D.Lgs 81/08 -D.lgs 106/09)

Protezione fisica delle aree e dei locali

- UPS Gruppi di continuità per PC
- UPS per le linee telefoniche
- Protezione degli archivi cartacei e conservazione sicura dei supporti di memorizzazione (disco rigido rimovibile, cd/dvd, pen drive)
- Regole per il controllo degli accessi fisici ai locali dell'azienda

Misure di Sicurezza Adeguate – Art. 32

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti derivanti da:

Distruzione, Perdita o Modifica dei Dati

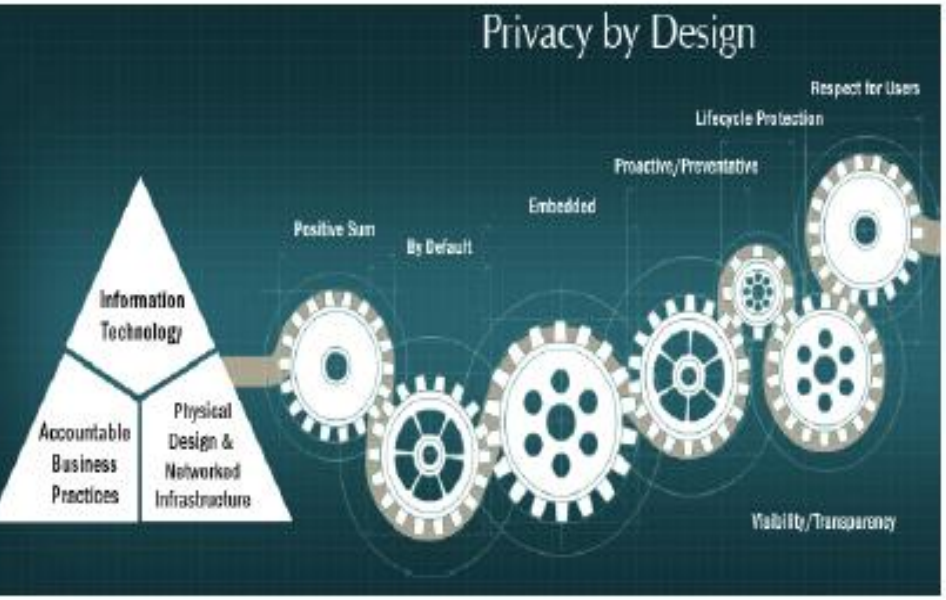
Divulgazione non autorizzata dei Dati

Accesso ai Dati in modo accidentale o illegale

Chiunque abbia accesso ai dati personali agisce sotto la responsabilità del Responsabile o dell'Incaricato del trattamento, e da essi è istruito in tal senso.

Privacy By Design e By Default – Art. 25

in dalla progettazione bisogna prevedere che le misure volte alla protezione dei dati personali
ano integrate nell'intero ciclo di vita tecnologico, dalla primissima fase di ideazione fino alla sua
ealizzazione, al suo utilizzo ed allo smaltimento finale.



Privacy By Design:
Individuazione di misure tecniche e organizzative adeguate per la protezione dei dati, già durante la fase di progettazione

Privacy By Default:
Garantire che siano trattati di default solo i dati personali necessari per ogni specifica finalità del trattamento

Pseudonimizzazione

Minimizzazione

Minimizzazione

Limitazione delle finalità

Integrazione delle garanzie a tutela dei diritti degli Interessati

Si potrà utilizzare un meccanismo di certificazione approvato per dimostrare la conformità del processo a tali requisiti.

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

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

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

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.

Gli obblighi di cui all'Art.30 non si applicano alle aziende con meno di **250 dipendenti**, tran
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

Data Breach Notification – Art. 33

Liberi PROFESSIONISTI
www.professionistiliberi.org

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

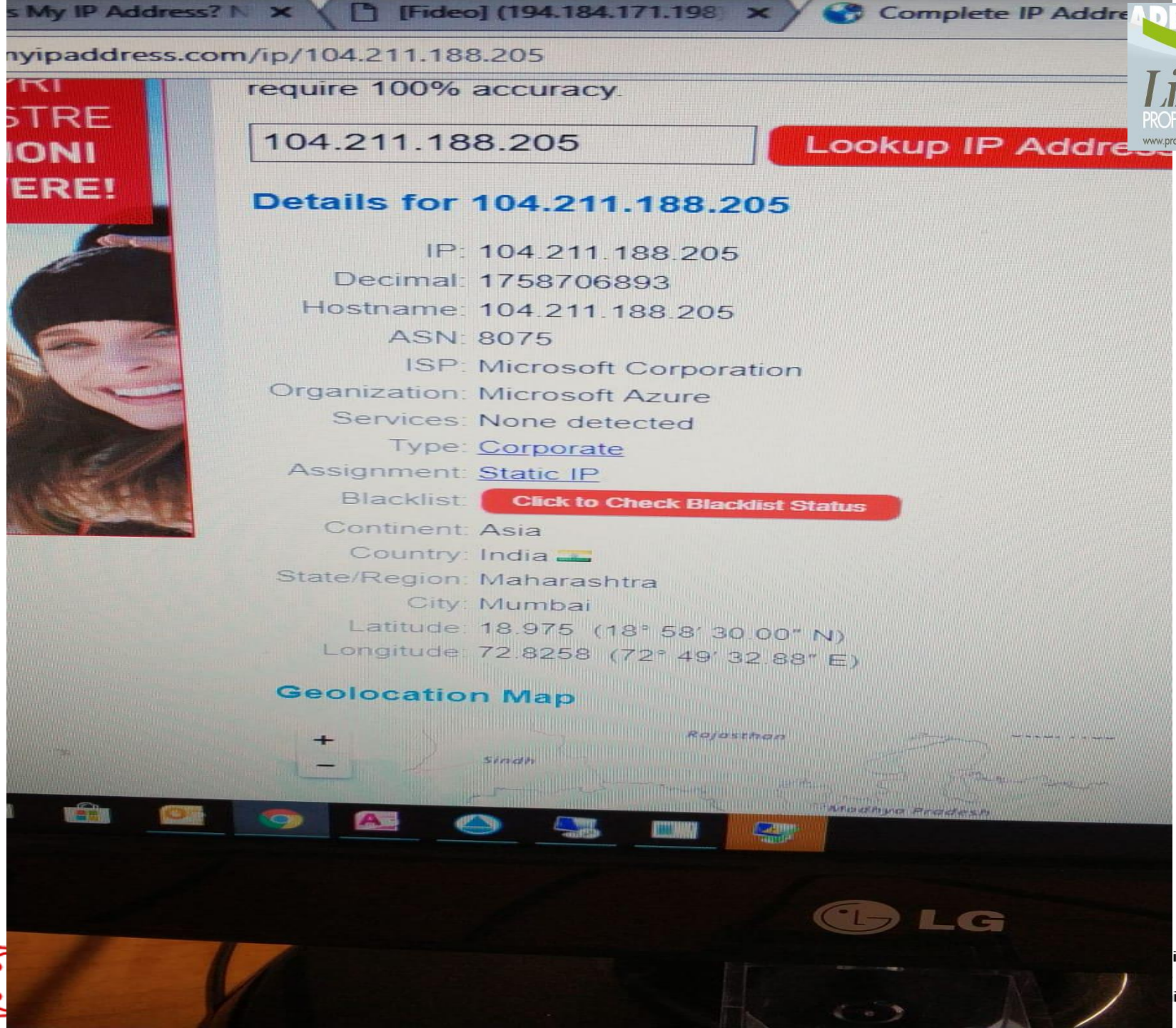
La comunicazione all'Interessato non è richiesta nei casi di:

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

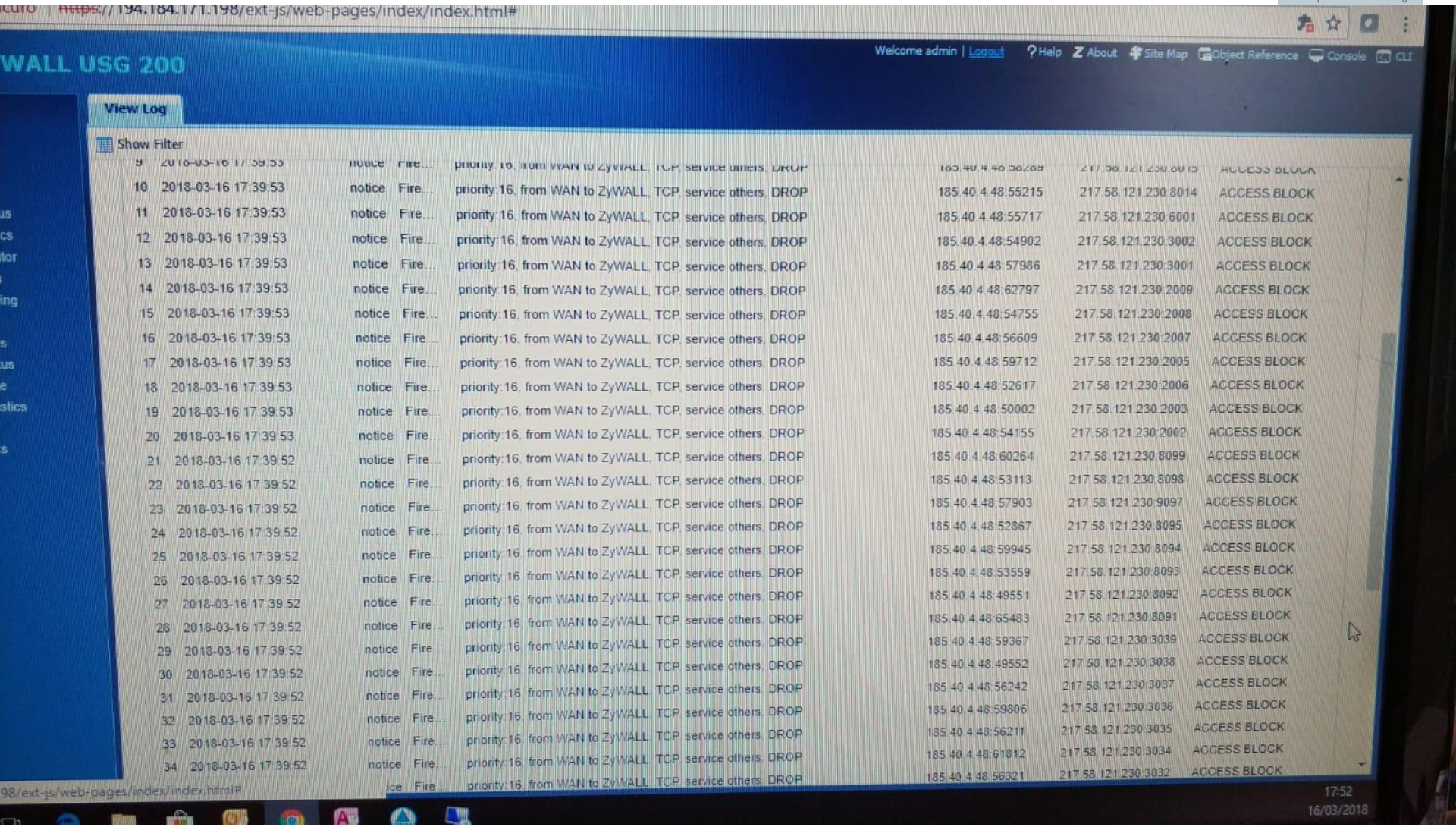
Successiva adozione di misure atte a scongiurare il sopraggiungere di rischi per i diritti e le libertà degli interessati

Comunicazione particolarmente difficoltosa o onerosa per il Responsabile

In questo caso occorre procedere a comunicazione pubblica o misura simile


My IP Address?
[Fideo] (194.184.171.198
Complete IP Addre
yipaddress.com/ip/104.211.188.205
require 100% accuracy.
104.211.188.205
Lookup IP Addres
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

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org



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.

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

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

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

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

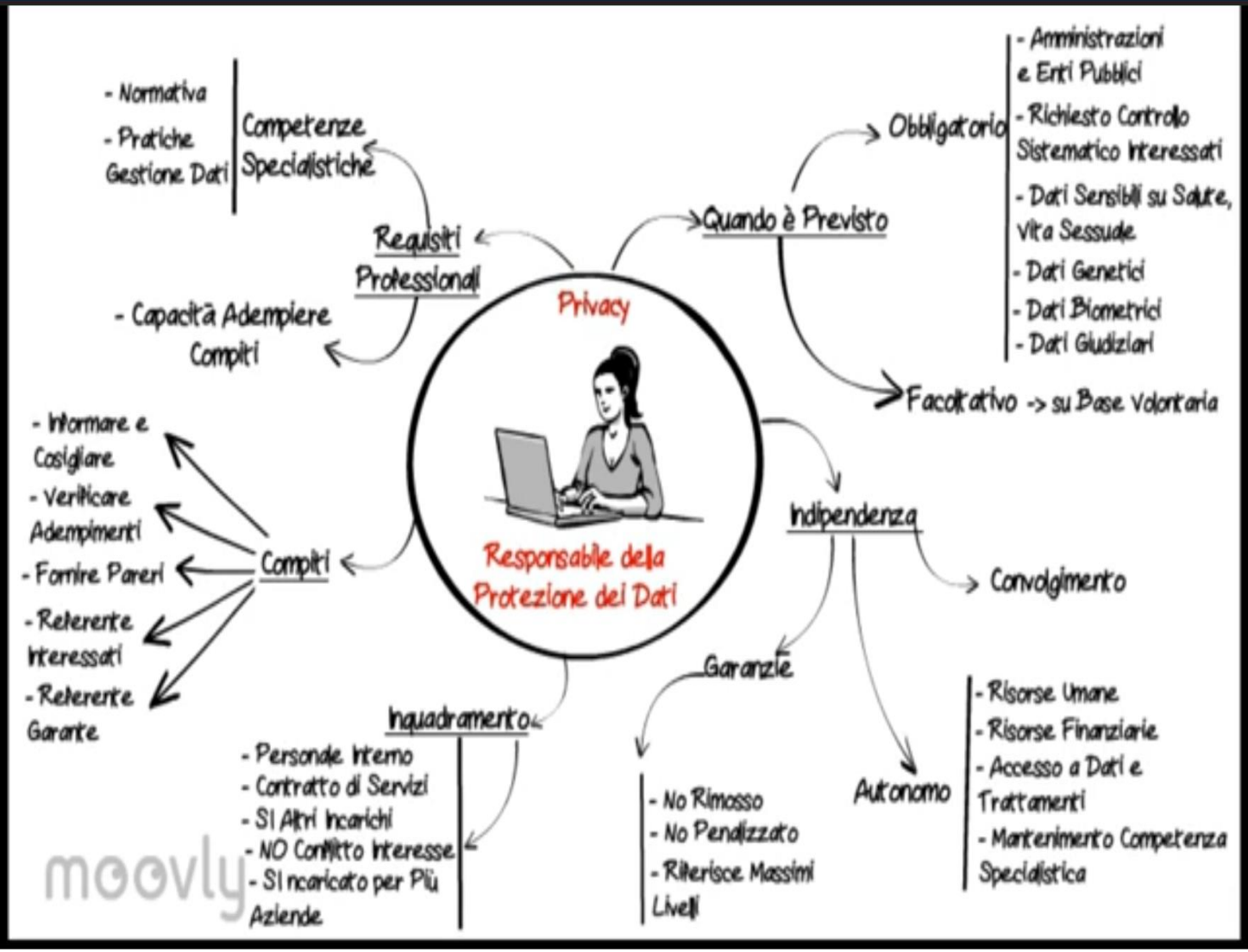
Analisi, Audit e Consultazioni

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.


Privacy
Responsabile della Protezione dei Dati
Requisiti Professionali
- Normativa
- Pratiche Gestione Dati
Competenze Specialistiche
- Capacità Adempiere Compiti
Quando è Previsto
Obbligatorio
- Amministrazioni e Enti Pubblici
- Richiesto Controllo Sistematico Interessati
- Dati Sensibili su Salute, Vita Sessuale
- Dati Genetici
- Dati Biometrici
- Dati Giudiziari
Facoltativo -> su Base Volontaria
Compiti
- Informare e Consigliare
- Verificare Adempimenti
- Fornire Pareri
- Referente Interessati
- Referente Garante
Indipendenza
Coinvolgimento
Garanzie
Inquadramento
- Persona Interno
- Contratto di Servizi
- SI Altri Incarichi
- NO Conflitto Interesse
- SI Incaricato per Più Aziende
- No Rimosso
- No Penalizzato
- Riferisce Massimi Livelli
Autonomo
- Risorse Umane
- Risorse Finanziarie
- Accesso a Dati e Trattamenti
- Mantenimento Competenza Specialistica
moovly

New

Il Data Protection Officer (4/4)
COMPITI

"Piccolo Garante" in Azienda

- **INFORMAZIONE E CONSULENZA**
  - Al Titolare, al Responsabile , agli Incaricati in merito ai loro obblighi
- **SORVEGLIANZA**
  - In merito all'osservanza del Regolamento e delle Policies aziendali e l'attribuzione delle responsabilità;
    - ✓ quindi: il rispetto dei diritti dell'interessato Informativa, Consenso, Accesso ai dati/ delle Misure di sicurezza/ della Notifica delle violazioni/ del principio di privacy by design/ della valutazione di impatto / della conservazione della documentazione, l'effettuazione dei controlli...)
  - Sensibilizza il personale e ne cura la formazione, inclusi gli auditors
- **SUPPORTO E INDIRIZZO**
  - Fornisce, se richiesto, parere in merito alla Valutazione di Impatto e ne sorveglia il seguito
- **RELAZIONI CON ESTERNO**
  - Coopera col Garante: le sue coordinate devono essere notificate
  - Punto di contatto con gli Interessati- coordinate nell'Informativa

ADERISCO Liberi PROFESSIONISTI www.professionistiliberi.org

Sanzioni – Art. 84

Il testo di Regolamento Europeo, rafforzato dal Parlamento Europeo, prevede sanzioni amministrative pecuniarie particolarmente elevate, anche proporzionate al volume di affari realizzato da una società, e dissuasive soprattutto per i Big Data.

Fino a 10.000.000 di € o

del fatturato mondiale annuo

- Violazioni degli obblighi del Responsabile e dell'Incaricato del Trattamento
- Violazione degli obblighi dell'organismo di certificazione
- Violazione degli obblighi dell'organismo di controllo

Fino a 20.000.000 di € o

del fatturato mondiale annuo

- Mancata osservanza di un ordine da parte dell'Autorità di controllo
- Violazione di nome su consenso, trasferimento verso paesi terzi e diritti degli interessati
- Mancata osservanza di leggi degli Stati membri

Il legislatore prevede un avvertimento scritto o una serie di verifiche periodiche presso il Responsabile, qualora questi abbia violato le norme per la prima volta e in caso di semplice colpa.

INADEMPIMENTO	D.lgd 101/2018
Omessa o inidonea informativa All'interessato. (Art. 161)	ABROGATO
Assenza informativa nei casi di dati sensibili o giudiziari o in caso di trattamenti che presentano rischi specifici o di maggiore rilev	ABROGATO
Omessa o incompleta notificazione al Garante Privacy. (Art.163)	ABROGATO
Omessa informazione o esibizione di documenti richiesti dal garante Privacy. (Art.164)	ABROGATO
Trattamento illecito di dati personali. (Art. 167 c.1.)	**Reclusione da 6 mesi a 1 e 6 mesi**. La pena è diminuita se il Garante ha riscosso la sanzione amministrativa
Trattamento illecito di dati personali. (Art. 167 c.2)	**Sanzione penale**, reclusione da **1 a 3 anni**.
Art. 167-*bis* *c.1. (Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*	**Arresto fino a 1 a 2 anni o**

INADEMPIMENTO	SANZIONE
Art. 167-*bis* c.2 *(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala)*	**Reclusione da 1 a 6 anni**
Art. 167-*ter (Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)*	**Reclusione da 1 a 6 anni**
Falsità nelle dichiarazioni al Garante Privacy.(Art. 168)	**Sanzione penale**, reclusione da **6 mesi a 3 anni**.
Omessa adozione di misure necessarie alla sicurezza dei dati.(Art. 169)	**ABROGATO**
Art. 170 (*Inosservanza di provvedimenti del Garante)*	**Sanzione penale**, reclusione da 3 **mesi a 2 anni**.

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è **punito con la reclusione da sei mesi a un anno e sei mesi.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al rattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-*sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2- septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2- quinquiesdecies arreca nocumento all'interessato****, è punito con la reclusione da uno a*** **tre anni.**

CAPO III – Illeciti Penali
Art. 167 (*Trattamento illecito di dati)*

- 3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli
- 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
- 6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

CAPO III – Illeciti Penali

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

- 1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-*ter, 2-sexies e 2-octies, è punito* **con la reclusione da uno a sei anni.**

- 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, **è punito con la reclusione da uno a sei anni,** quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

ADERISCO
Liberi PROFESSIONISTI
www.professionistiliberi.org

CAPO III – Illeciti Penali
Art. 167–*ter*(*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala)*

c.1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è pun**ito con la reclusione da uno a quattro anni.**

1 a 4 anni

CAPO III – Illeciti Penali

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

C 1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con **la reclusione da sei mesi a tre anni.**

C 2. Fuori dei casi di cui al comma 1, è punito con la **reclusione sino ad un anno** chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.

CAPO III – Illeciti Penali

Art. 170 (*Inosservanza di provvedimenti del Garante)*

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

3 mesi a 2 anni

Reati informatici

- Reati compiuti per mezzo o nei confronti di un sistema informatico. L'illecito può consistere nel sottrarre o distruggere le informazioni contenute nella memoria del personal computer. In altri casi, invece, il computer concretizza lo strumento per la commissione di reati, come nel caso di chi utilizzi le tecnologie informatiche per la realizzazione di frodi. La prima normativa contro i cyber crimes L. 547/1993:

- Frode informatica (art. 640): consiste nell'alterare un sistema informatico allo scopo di procurarsi un ingiusto profitto (Phishing)
- Accesso abusivo a un sistema informatico o telematico (art. 615 ter) : condotta di colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza o vi si mantiene contro la volontàdi chi ha il diritto di escluderlo o violando le prescrizioni del titolare del sistema.
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici (art. 614 quater c.p.) : al fine di procurare a sé o ad altri un profitto o di arreca ad altri un danno, riproducendo, diffondendo, comunicando o consegnando codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni idonee

-

Reati informatici

- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615 quinquies) chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione o l'alterazione.
- Intercettazione, impedimento o interruzione illecita di comunicazioni (artt. 617 quater e 617 quinquies) chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui che installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni informatiche.
- Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi (art. 617 sexies) Chi falsifica, altera o sopprime la comunicazione informatica acquisita e chi distrugge, deteriora, cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.).
-

L' ATTIVITA' ISPETTIVA (1)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

DIPARTIMENTO ATTIVITA' ISPETTIVE

Prot. n.

Roma,

Oggetto: *Richiesta di informazioni ai sensi dell'art. 58, comma 1, lettera a) ed e), del Regolamento generale sulla protezione dei dati (UE) 2016/679 (di seguito Rgdp) e dell'art. 157 e 158 del decreto legislativo n. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) (di seguito Codice).*

Con riferimento al trattamento di dati personali effettuato
si invita il soggetto in indirizzo, ai sensi dell'art. 58, c. 1, lettera a) ed e), del *Rgdp* e dell'art. 157 e 158 del *Codice*, a comunicare all'organo incaricato di notificare la presente richiesta:

1) struttura ed organizzazione della società;
2) distribuzione delle funzioni in materia di protezione dei dati personali;
3) modalità con la quale viene fornita agli interessati l'informativa di cui agli art. 13 e 14 del *Rgdp* acquisendo copia della relativa documentazione;
4) modalità di acquisizione dei consensi ai sensi degli artt. 7 e 8 del *Rgdp*, per le ulteriori finalità (*marketing* – profilazione – comunicazione dei dati a soggetti terzi) con relativa documentazione;

L' ATTIVITA' ISPETTIVA (2)

5) eventuale istituzione del registro dei trattamenti mettendone a disposizione copia dello stesso (art. 30 *Rgdp*);
6) eventuale designazione di responsabili esterni (e/o *sub* responsabili) del trattamento con acquisizione del relativo contratto e designazione (art. 28 del *Rgdp*);
7) eventuale nomina del DPO in relazione agli artt. 37 e segg. del *Rgdp*;
8) soggetti autorizzati ad accedere ai dati personali oggetto del trattamento e documentazione relativa all'istruzione ed alla formazione degli incaricati ed eventuale copia delle nomine a incaricati (art. 29 *Rgdp*);
9) tipologia di profilazione effettuata e descrizione dettagliata del suo funzionamento, con particolare riferimento alle modalità di raccolta, di aggregazione e di analisi dei dati personali della clientela;
10) eventuale utilizzo a fini di profilazione di dati particolari dell'interessato (art. 9 *Rgdp*);
11) tipologia di attività di *marketing* effettuato a seguito della profilazione;
12) il periodo di conservazione dei dati di profilazione personali ovvero i criteri utilizzati per determinare tale periodo;
13) valutazione d'impatto eventualmente effettuata in relazione ai trattamenti dei dati oggetto della profilazione tenendo conto di quanto previsto al riguardo nella delibera del Collegio datata 11 ottobre 2018 (*vgs. doc. web.* 9058979) fornendo gli elementi di tale valutazione;

Piazza di Monte Citorio, 121 - 00186 Roma
Tel. +39 06 696772794 - Fax +39 06 696773785
www.garanteprivacy.it
E-mail: dais@gpdp.it
Posta certificata: dais@pec.gpdp.it

Question Time

Dr. DAVIDE CANDIA

- Dottore Commercialista – Revisore 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


grazie