99 Articoli
173 Considerando

Corso Aziendale G.D.P.R. LINEA COMPUTERS SRL
Sulla Protezione del Dato e sue Conformità

AGENDA:

.18:00 INTRODUZIONE ALLA GIORNATA E AI RELATORI

OBIETTIVI DEL CORSO: COMPRENDERE GLI ASPETTI FONDAMENTALI DEL GDPR

.18:10 PIATTAFORMA ODOO PER ESAME FINALE

PRIMA PARTE - PRINCIPI DI BASE DEL GDPR

PROTEZIONE DEI DATI PERSONALI E DIRITTI DELL'INDIVIDUO.
PRINCIPI FONDAMENTALI DEL GDPR:
ACCOUNTABILITY
TRATTAMENTO DATI
MARKETING
DATA BREACH
DPIA
PDCA

SECONDA PARTE - 18:40 ESEMPI PRATICI E VALUTAZIONI

. 19:15 ESAME LIVE (SMARTPHONE)

Relatori
Chi siamo

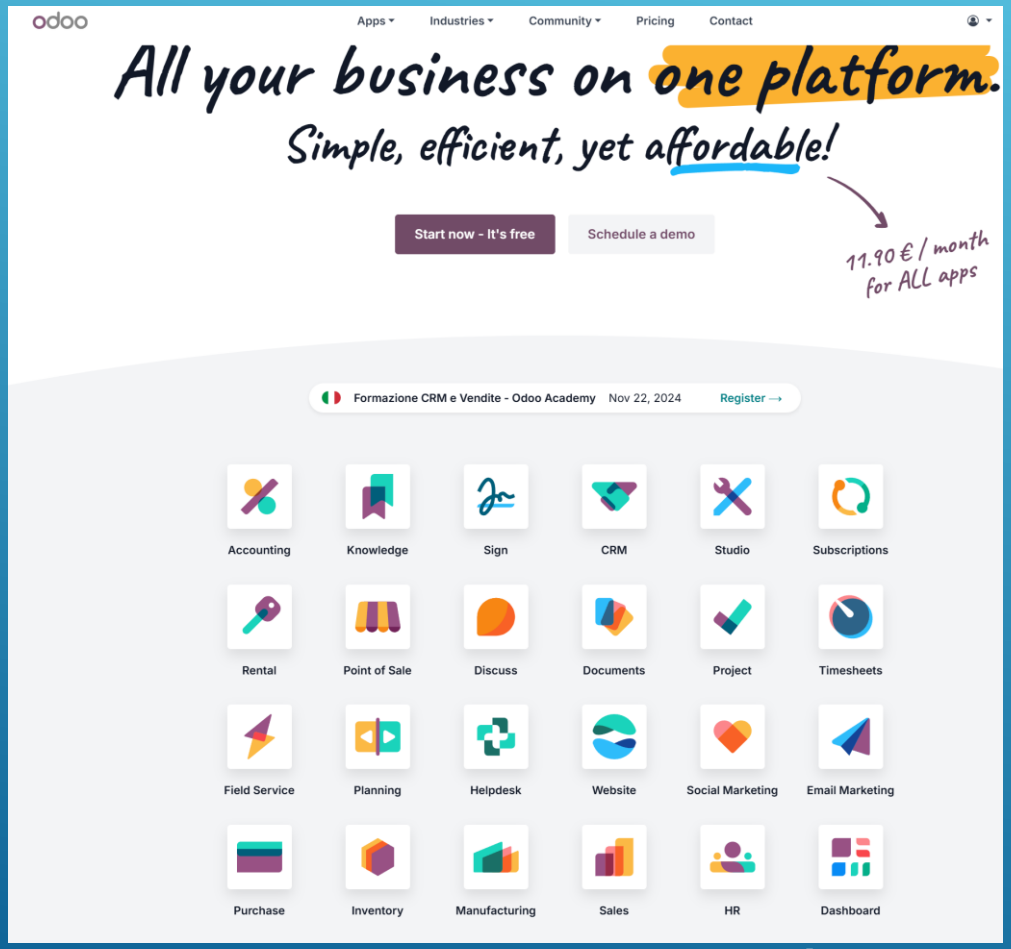
Privacy officer – Customer Service Department

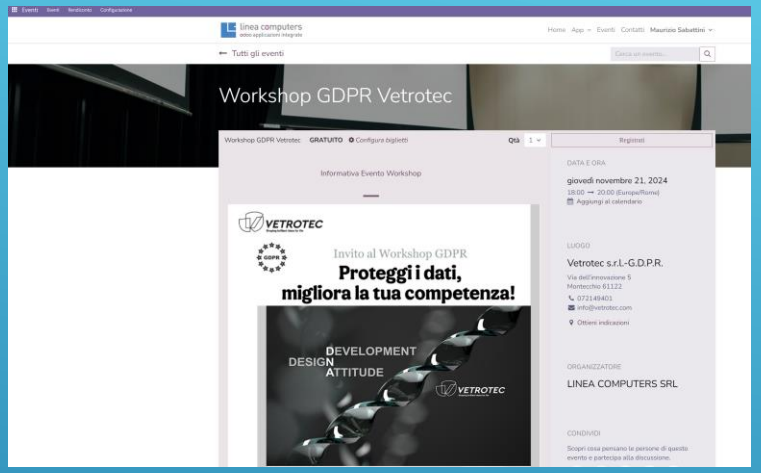
Software Developer

INFORMATICO CO-FOUNDER – CHIEF OPERATING OFFICER

Consulente Privacy Officer certificato TUV CDP_451
https://www.linkedin.com/in/maurizio-sabattini/

- **Piattaforma Odoo**
- **App >> Eventi - E-Learning - Esame Live - Firma - Documenti**

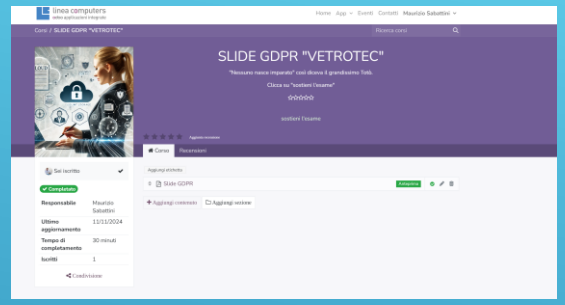




Eventi

www.odoo.com

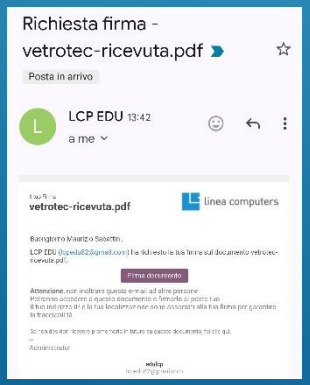
- **Piattaforma Odoo** **www.odoo.com**
- **App >> Eventi - E-Learning – Esame Live – Firma - Documenti**

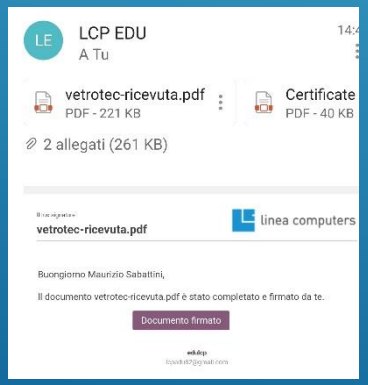


https://spazio.lineacomputers.com/slides/slide-gdpr-linea-computers-srl-3

https://spazio.lineacomputers.com/s/49401

70/100 punti per superamento





ATTESTATO DI PARTECIPAZIONE
Ricevuta consegna

Perché un workshop sul GDPR?

- ✓ Obblighi di legge
- ✓ Prevenzioni incidenti 80% errore umano
- ✓ Protezione per l'azienda
- ✓ Reputazione azienda
- ✓ Sanzioni
- ✓ Maggior consapevolezza dei diritti dei dipendenti
- ✓ Casi pratici

1890, La differenza tra protezione del dato e diritto alla privacy

Adesso immaginati Le prime automobili fine ‘800. Ci sono ancora le carrozze. Niente TV. La tecnologia più avanzata in *campo media* è la fotografia. Il mezzo di comunicazione più diffuso è la stampa.

Oggi lo chiameremmo **trattamento e diffusione di dati su Larga scala**.

Non è la tecnologia di per sé, ma **L’USO CHE SE NE FA** a creare un problema per i singoli individui.

Privacy e protezione del dato non sono la stessa cosa.

NEL 1981, il Consiglio d’Europa adotta la Convenzione 108, un concetto legato al **diritto alla libertà**.
Una libertà che va protetta da un controllo esterno (da parte di privati o da parte dello Stato)

Se Antonio a casa sua gira in mutande, con la cuffia da doccia rosa in testa e la giarrettiera, sono fatti suoi, è la sua privacy. Se per lavoro Antonio deve comprare un biglietto del treno per andare da Pesaro a Milano, dove sopra c’è scritto come si chiama, a che ora parte , posto a sedere, è un trattamento di dati personali.

Google, Facebook, Amazon sono **poteri privati**: società private che hanno un potere enorme sulla nostra identità digitale.

Che cos'è il GDPR? (EU) 2016/679

Definizione: Regolamento Generale sulla Protezione dei Dati

Ambito: Applicabile nell'UE e a tutte le aziende che trattano i dati di cittadini UE

Entrata in vigore: 25 maggio 2018

https://www.garanteprivacy.it/il-testo-del-regolamento

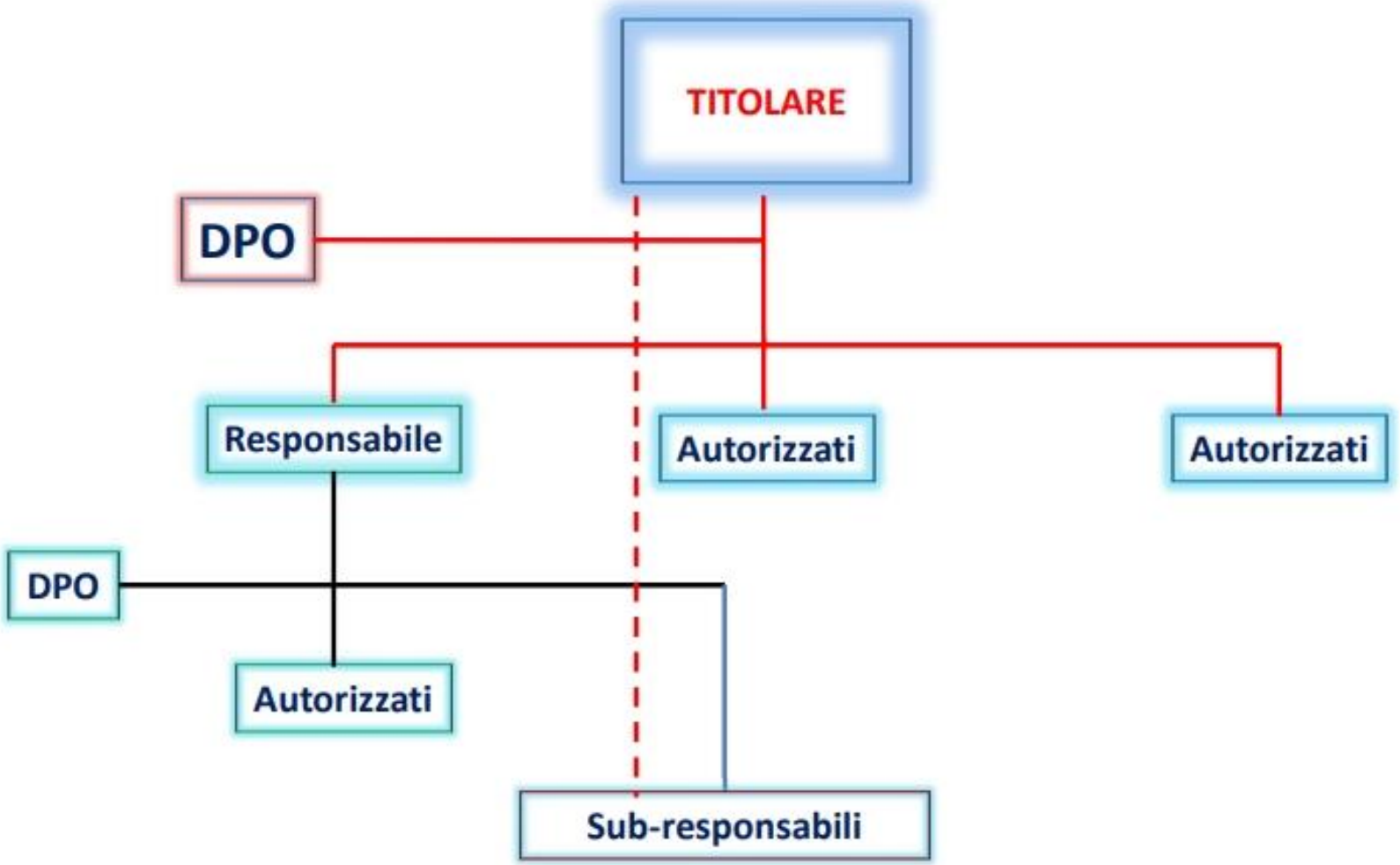
Cosa vuol dire essere COMPLIANT al GDPR?

Essere **COMPLIANT** → **AGIRE CON ACCOUNTABILITY.**

Essere **COMPLIANT** → essere **CONFORMI al GDPR**

Significa che il titolare del trattamento, tutti i responsabili/incaricati, devono essere formati ed informati su cosa prevede il Regolamento e su come comportarsi per proteggere i dati personali.

ORGANIGRAMMA PRIVACY SECONDO IL GDPR



Per "**DATO PERSONALE**" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo

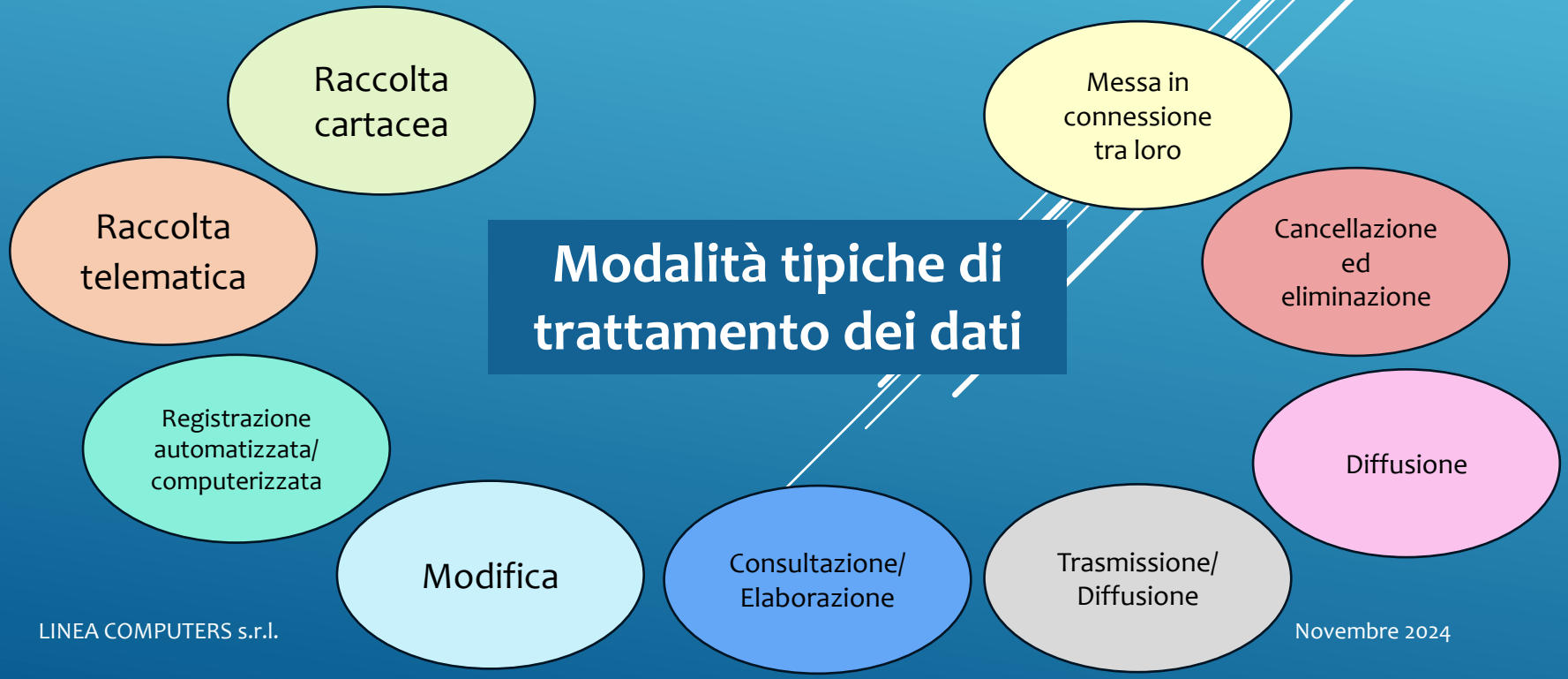
Alcuni esempi di dati identificativi da proteggere

nome e cognome
indirizzo (di casa)
indirizzo email (nome.cognome@dominio)
numero di telefono cellulare personale
codice fiscale
Iban
numero di targa del veicolo
numero di patente
data e luogo di nascita
genere (maschio o femmina)

IL TRATTAMENTO DEI DATI

UN'ASSOCIAZIONE/ENTE, PER OPERARE E RAGGIUNGERE IL SUO SCOPO SOCIALE, DEVE FARE NECESSARIAMENTE USO DEI DATI RACCOLTI.

LA MODALITÀ D'USO DEI DATI È QUEL CHE GIURIDICAMENTE SI CHIAMA «**TRATTAMENTO**».



OGGI

Titolo

idpass3f84c05a-5d0d-4b43-a326-d082652525f0

IN PASSATO

Maurizio Sabattini

Email maurizio.sabattini@lineacomputers.com

Cellulare 348[redacted]

Ruolo Relatore

Posizione Sala A0

Cosa vuol dire ACCOUNTABILITY?

Accountability vuol dire **responsabilità.**

Accountable è l'azienda, l'ente, l'associazione o il professionista che tratta i dati personali con la consapevolezza che quelle informazioni non sono sue e che deve fare tutto il possibile perché non accada loro nulla di male.

È come quando saliamo sul **Frecciarossa**, che in fondo non è altro che una scatola di metallo che viaggia a 300 km orari. Saremmo dei pazzi a decidere consapevolmente di prendere un mezzo del genere, ma **noi ci fidiamo.**

Ci fidiamo di chi l'ha costruito, di chi fa la manutenzione, di chi fa le riparazioni, perché **sono accountable**: sono consapevoli del rischio che potrebbero correre i passeggeri se qualcosa dovesse andare storto e hanno progettato il treno e i sistemi di sicurezza per **ridurre i pericoli ai minimi termini**.

Quindi, per essere COMPLIANT → Bisogna agire con ACCOUNTABILITY

per AGIRE CON ACCOUNTABILITY → Bisogna essere: consapevoli, competenti e responsabili

RESPONSABILITÀ ALL'INTERNO DELL'AZIENDA
Chi è responsabile?

TUTTI I DIPENDENTI CHE TRATTANO DATI PERSONALI DEVONO RISPETTARE IL GDPR

Il Regolamento UE 679/16 ha 99 articoli, 11 capi e 173 considerando...99 articoli ne prendiamo in considerazione 3:

Art 5 - Art 6 - Art 15

ART. 5 Principi applicabili al trattamento di dati personali

Questo articolo è cruciale perché stabilisce i principi fondamentali per il trattamento dei dati personali, cui ogni organizzazione deve attenersi per essere conforme al regolamento.

1. **Liceità, correttezza e trasparenza**
   - Trattamento legittimo e chiaro verso l'interessato.
2. **Limitazione della finalità**
   - Dati raccolti per finalità specifiche e legittime.
3. **Minimizzazione dei dati**
   - Solo i dati strettamente necessari al fine.
4. **Esattezza**
   - Dati esatti e aggiornati, per evitare errori.
5. **Limitazione della conservazione**
   - Conservare solo per il tempo necessario alle finalità.
6. **Integrità e riservatezza**
   - Sicurezza e protezione da accessi non autorizzati.

Principio di responsabilità: Il titolare del trattamento è responsabile della conformità a questi principi e deve poterlo dimostrare.

ART. 6 Liceità del trattamento

Cosa significa "liceità"?

Significa che non possiamo raccogliere, usare o conservare i dati personali a nostro piacimento. Dobbiamo avere una giustificazione legale. Le basi giuridiche più comuni sono:

1. **Consenso** dell'interessato.
2. **Esecuzione di un contratto**.
3. **Obbligo legale**.
4. **Interessi vitali** dell'interessato o di un'altra persona.
5. **Interesse pubblico** o esercizio di pubblici poteri.
6. **Legittimo interesse** del titolare del trattamento.

Immaginate di andare in una **palestra**.
Per iscrivervi, compilate un modulo con dati personali come nome, cognome, numero di telefono ed eventualmente dati sanitari (ad esempio, certificato medico).

- **Perché la palestra può trattare i vostri dati?**
  La base giuridica qui è **l'esecuzione di un contratto**.
  Senza quei dati, la palestra non potrebbe:
  - creare il vostro abbonamento;
  - contattarvi per comunicazioni importanti (ad esempio, modifiche agli orari).

E se vi chiedessero il numero di scarpe?
Questo dato **non è necessario** per il contratto. Se richiesto, non avrebbe una base giuridica valida e sarebbe una violazione del principio di liceità e minimizzazione

ART. 15 Diritto di accesso dell'interessato

Cos'è il diritto di accesso?

Ogni persona ha il diritto di:

1. **Sapere se i suoi dati vengono trattati**.
2. **Ottenere una copia dei dati personali trattati**.
3. **Ricevere informazioni chiare e trasparenti** sul trattamento, come:
    - Lo scopo del trattamento.
    - Le categorie di dati raccolti.
    - I destinatari dei dati (es. altre aziende o enti).
    - Il periodo di conservazione.

Immaginate di essere clienti di un negozio online, dove avete acquistato un prodotto. Dopo qualche mese, decidete di esercitare il **diritto di accesso** e inviate un'email chiedendo: *"Vorrei sapere quali dati personali avete su di me e come li state usando."*

Cosa deve fare il negozio?
Rispondere entro 30 giorni: Deve confermare se sta trattando i vostri dati.
Fornire una copia dei dati: Ad esempio, storico degli acquisti, indirizzo di spedizione, e-mail registrata.
Spiegare il trattamento: Deve chiarire perché conserva i dati, ad esempio:
Per la consegna degli ordini (esecuzione di un contratto).
Per inviare promozioni (se avete dato il consenso).

COME FARE **EMAIL MARKETING** IN AZIENDA RISPETTANDO LA **PRIVACY**

Consenso esplicito degli utenti

Prima di inviare email promozionali, raccogli il **consenso esplicito** tramite un **modulo di iscrizione** chiaro e trasparente.

Esempio: "Iscriviti alla nostra newsletter. Acconsento al trattamento dei miei dati personali per ricevere comunicazioni commerciali."

Interesse Legittimo dell'azienda

In alcuni casi, puoi inviareemail marketing basandoti sull'**interesse legittimo** dell'azienda (**Soft Opt-In**)

Esempio: Puoi inviare offerte a clienti esistenti per prodotti simili a quelli già acquistati, se non si oppongono al trattamento.

! Attenzione: Devi comunque garantire che l'utente possa facilmente esercitare il diritto di opposizione, ovvero di rinunciare a ricevere ulteriori comunicazioni.

SOFT OPT-IN

- Immagina un cliente che acquista una t -shirt da un negozio online. L'azienda raccoglie il suo indirizzo email durante l'acquisto e, in futuro, **invia email promozionali con offerte per t -shirt o altri articoli di abbigliamento**. L'azienda può farlo senza ottenere un consenso esplicito per ogni singola email, ma **deve includere sempre un'opzione facile per disiscriversi dalla lista**.

Limiti del Soft Opt-In:

- Non si applica se l'azienda raccoglie l'email in modo indiretto (ad es: tramite una lista di terze parti).
- Non si applica se l'azienda invia offerte per **prodotti non correlati** a quelli già acquistati dal cliente.
- È necessario che l'azienda fornisca sempre l'opzione di **disiscrizione**.

Il soft opt-in consente alle aziende di inviare comunicazioni promozionali ai propri clienti esistenti senza necessitare un consenso esplicito, ma **solo per prodotti simili a quelli già acquistati**, purché vengano rispettati i diritti dell'utente di **disiscriversi facilmente** e vengano rispettati i **principi di trasparenza** e **minimizzazione dei dati**.

Cos'è la DPIA?

La DPIA è uno strumento fondamentale previsto dal **GDPR** (Art. 35) per identificare e mitigare i rischi legati alla protezione dei dati personali, particolarmente utile in caso di trattamenti ad alto rischio.

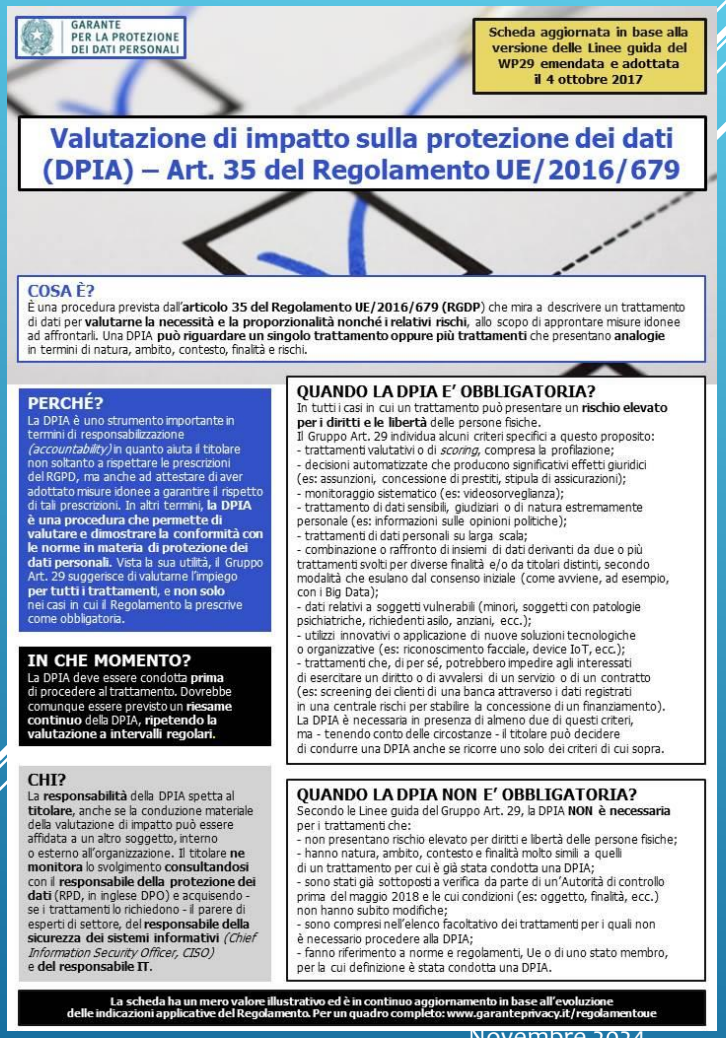
OBBIETTIVI PRINCIPALI:

1. **Identificare i rischi** per i diritti e le libertà degli interessati.

2. **Definire misure** per mitigare tali rischi.

3. **Dimostrare la conformità** con il GDPR.

DPIA: Anticipa i rischi, proteggi i dati, rispetta la legge!



GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?
È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?
La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?
La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?
La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

QUANDO LA DPIA E' OBBLIGATORIA?
In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

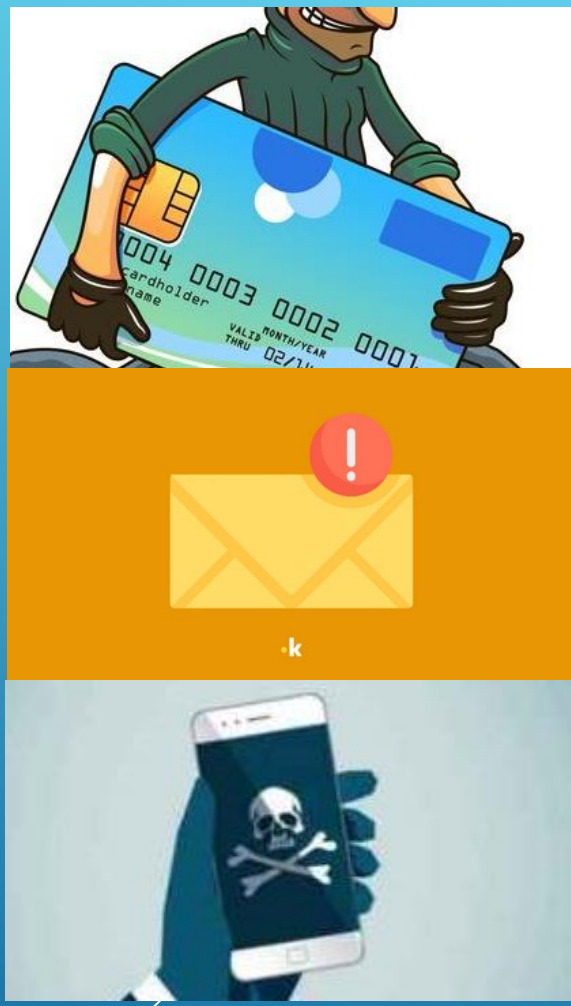
QUANDO LA DPIA NON E' OBBLIGATORIA?
Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

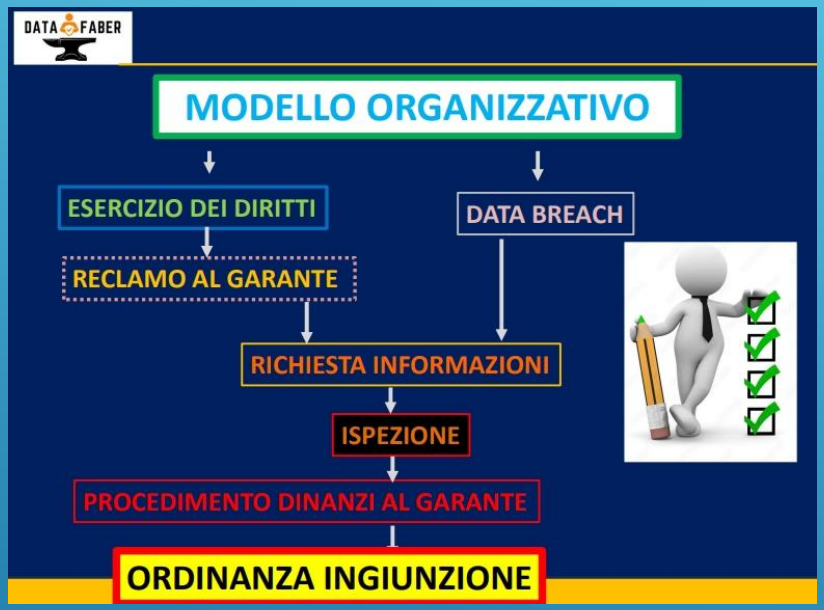
COS'È UNA VIOLAZIONE DEI DATI?
DEFINIZIONE:

LA VIOLAZIONE DEI DATI SI VERIFICA IN CASO DI:
- **PERDITA**
- **ACCESSO NON AUTORIZZATO**
- **DIVULGAZIONE DI DATI PERSONALI**

ESEMPI DI VIOLAZIONE:
- **FURTO DI DATI,**
- **ERRORI UMANI,**
- **ACCESSO NON AUTORIZZATO AI DATI**



DEFINIZIONE DI **DATA BREACH** (ART. 4) 20 «VIOLAZIONE DEI DATI PERSONALI»: LA VIOLAZIONE DI SICUREZZA CHE COMPORTA ACCIDENTALMENTE O IN MODO ILLECITO LA DISTRUZIONE, LA PERDITA, LA MODIFICA, LA DIVULGAZIONE NON AUTORIZZATA O L'ACCESSO [NON AUTORIZZATO] AI DATI PERSONALI TRASMESSI, CONSERVATI O COMUNQUE TRATTATI.



Cause frequenti:

- **Errore umano (Errori nella gestione,**
- **compromissione backup,**
- **perdita di una chiavetta usb..)**
- **Attacchi (Virus & Malware, accesi abusivi,..)**
- **Danni e hardware**
- **Fornitura di energia**
- **Eventi naturali**

Art. 33 GDPR 27 Notifica di una violazione dei dati personali all'autorità di controllo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Perché è importante il GDPR?

Il GDPR tutela la privacy dei cittadini e garantisce che le persone abbiano un controllo sui propri dati personali.

Conseguenze per le aziende:
Multe elevate e danni alla reputazione.

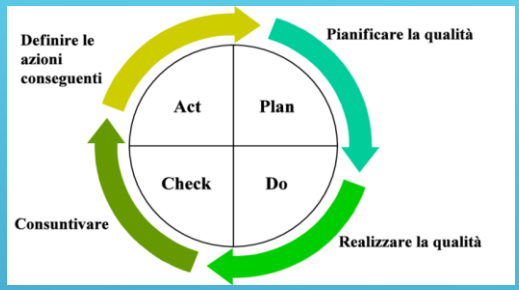
1.**Fino a 10 milioni di euro o al 2% del fatturato annuo globale** (si applica l'importo maggiore):

1. Mancata notifica delle violazioni dei dati personali entro 72 ore.
2. Assenza di misure tecniche e organizzative adeguate per proteggere i dati.
3. Incapacità di tenere registri del trattamento dei dati.
4. Non nominare un responsabile della protezione dei dati (DPO) se richiesto.

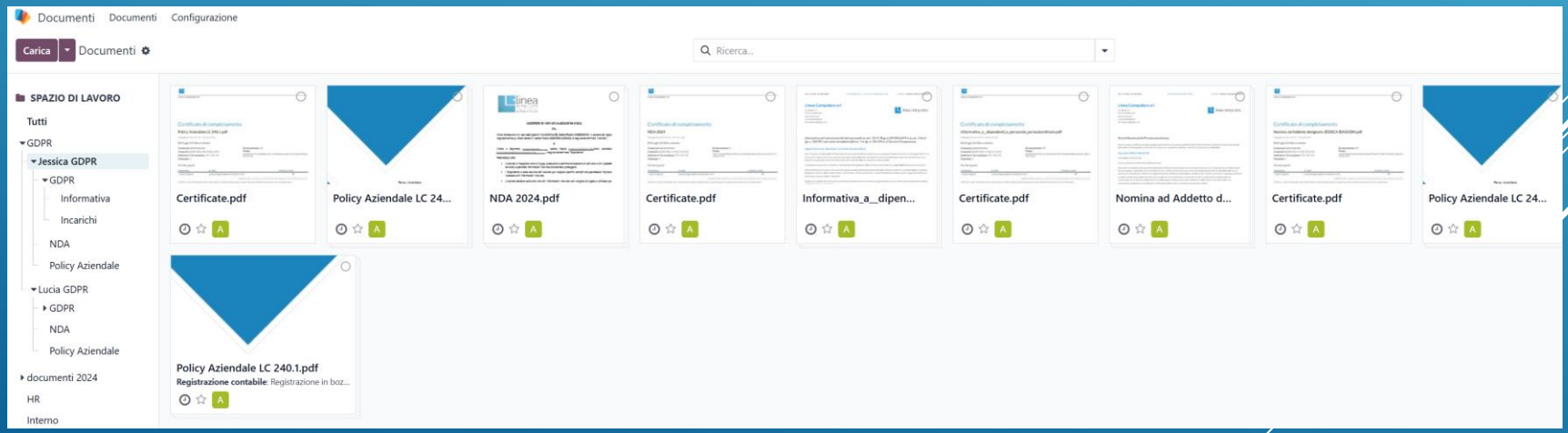
2.Fino a 20 milioni di euro o al 4% del fatturato annuo globale (si applica l'importo maggiore):

1. Trattamento dei dati personali senza una base giuridica valida.
2. Violazione dei diritti degli interessati e portabilità.
3. Mancato rispetto dei principi fondamentali di protezione dei dati come trasparenza, minimizzazione dei dati e sicurezza.

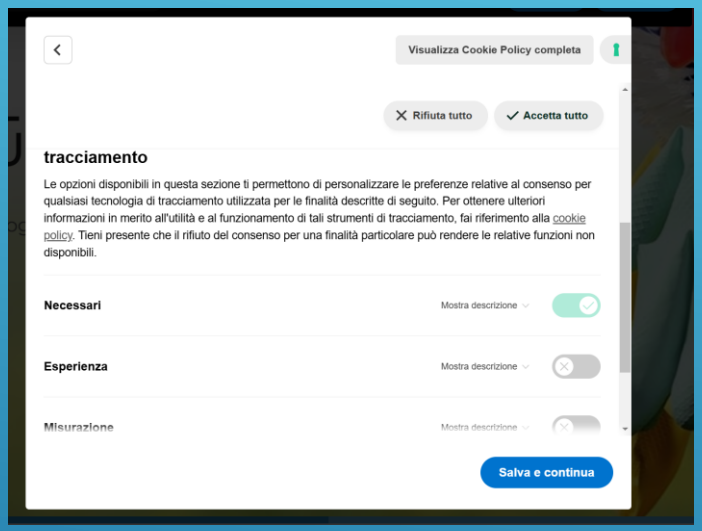
Miglioramento del ciclo continuo della Privacy
Ciclo di deming (PDCA)

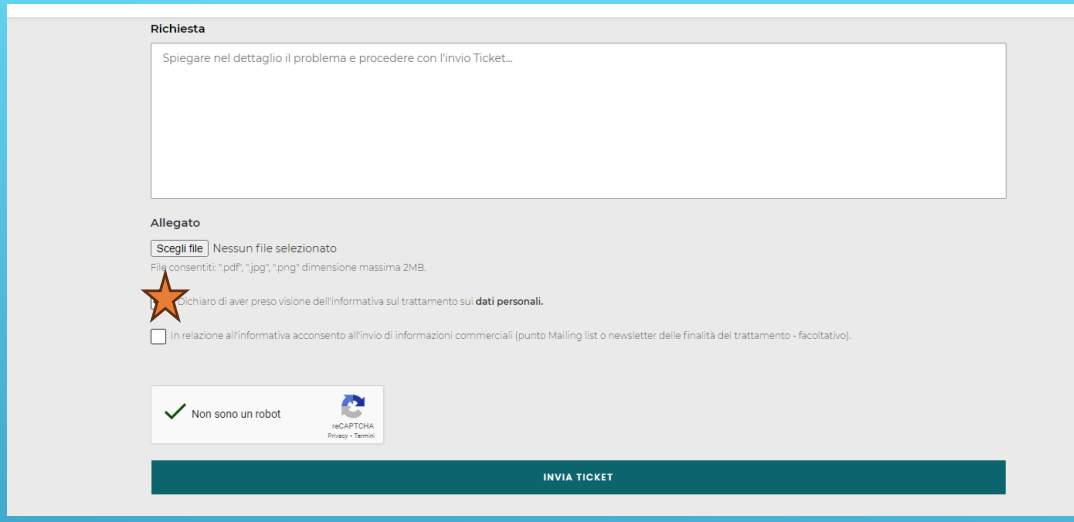


° M.O.P. modello organizzativo Privacy
° Policy Aziendale
° Mansionario

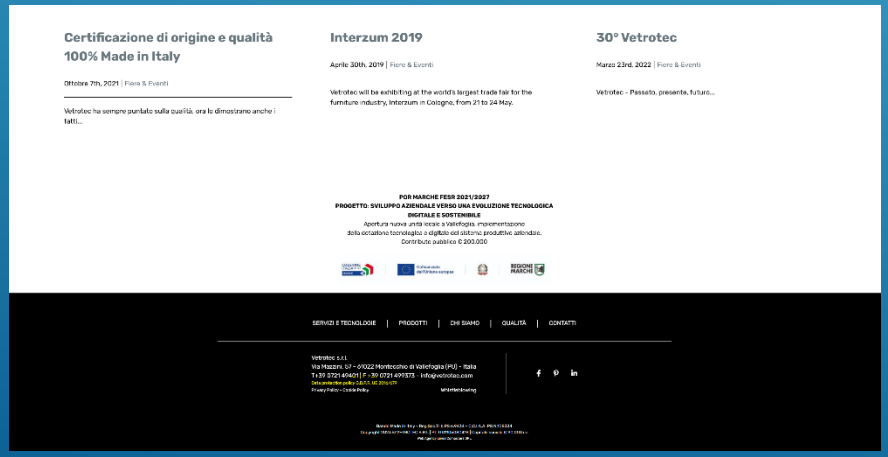


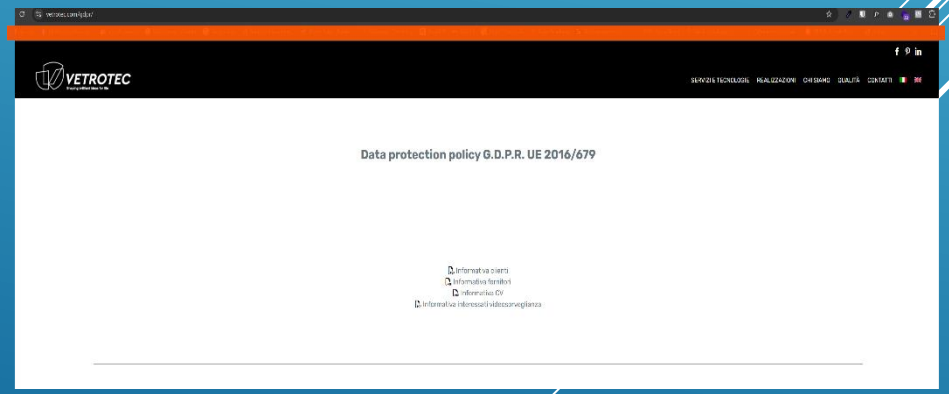

Your current compliance rating
50%
iubenda for WordPress
The all-in-one solution
to make your website compliant!
NEW
Now with scanning and auto-configuration


Visualizza Cookie Policy completa
Rifiuta tutto
Accetta tutto
tracciamento
Le opzioni disponibili in questa sezione ti permettono di personalizzare le preferenze relative al consenso per qualsiasi tecnologia di tracciamento utilizzata per le finalità descritte di seguito. Per ottenere ulteriori informazioni in merito all'utilità e al funzionamento di tali strumenti di tracciamento, fai riferimento alla cookie policy. Tieni presente che il rifiuto del consenso per una finalità particolare può rendere le relative funzioni non disponibili.
Necessari
Mostra descrizione
Esperienza
Mostra descrizione
Misurazione
Mostra descrizione
Salva e continua


Richiesta
Spiegare nel dettaglio il problema e procedere con l'invio Ticket...
Allegato
Scegli file
Nessun file selezionato
File consentiti: *.pdf, *.jpg, *.png dimensione massima 2MB.
Dichiaro di aver preso visione dell'informativa sul trattamento sui dati personali.
In relazione all'informativa acconsento all'invio di informazioni commerciali (punto Mailing list o newsletter delle finalità del trattamento - facoltativo).
Non sono un robot
reCAPTCHA
Privacy - Termini
INVIA TICKET

WEB SITE


Certificazione di origine e qualità
100% Made in Italy
Ottobre 7th, 2021 | Fiere & Eventi
Interzum 2019
Aprile 30th, 2019 | Fiere & Eventi
Vetrotec will be exhibiting at the world's largest trade fair for the furniture industry, interzum in Cologne, from 21 to 24 May.
30° Vetrotec
Marzo 23rd, 2022 | Fiere & Eventi
Vetrotec - Passato, presente, futuro...
POR MARCHE FESR 2021/2027
PROGETTO: SVILUPPO AZIENDALE VERSO UNA EVOLUZIONE TECNOLOGICA DIGITALE E SOSTENIBILE
Apertura nuova unità locale a Valleoglia. Implementazione della iocalizzazione tecnologica e digitale ed sistema produttivo aziendale.
Contributo pubblico € 200.000
SERVIZI E TECNOLOGIE | PRODOTTI | CHI SIAMO | QUALITÀ | CONTATTI


VETROTEC
SERVIZI E TECNOLOGIE
REALIZZAZIONI
CHI SIAMO
QUALITÀ
CONTATTI
Data protection policy G.D.P.R. UE 2016/679

ESEMPI CONCRETI

PROTEZIONE DEL DATO
ACCOUNTABILITY

ART. 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49

ART. 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99

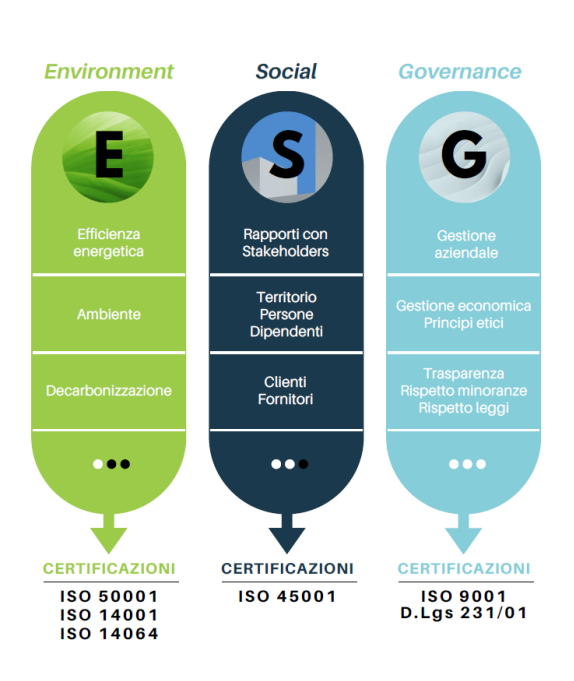
- INFORMATIVA
- INCARICHI
- DIPENDENTI
  - Decreto trasparenza 104/2022
- CLIENTI FORNITORI
  - INFORMATIVE
  - CONSENSI
  - RESP. ESTERNO
- ORGANIGRAMMA
  - Regolamento aziendale
  - Policy aziendale - strumenti informatici
- AUDIT FORNITORI
  - NOMINA
  - CONTRATTO CON CLAUSOLE
- CONTITOLARI

- Policy Aziendale
- M.O.P. Modello Organizzativo Privacy
- NIS 2 Direttiva (UE) 2022/2555
- AI ACT Regulation (EU) 2024/1689
- APPLICAZIONI
  - ERP
  - CRM
  - POSTA ELETTRONICA
  - HR
- SERVER
  - PC / TABLET
  - TELECAMERE
  - BADGE
- CARTELLE
  - ARMADI
  - DATABASE
  - CLOUD
- SITO WEB
  - COOKIE SOLUTION
  - COOKIE POLICY
  - PRIVACY POLICY
- Vulnerabilità Software - Hardware Verifica livelli di sicurezza interno ed esterno
- CYBER SECURITY
  - Cyber Threat Intelligence
- Modello organizzativo interno WHISTLEBLOWING
  - Informative
  - Nomina autorizzati
  - Registro trattamento
  - Nomina Resp. trattamento
  - DPIA
- TITOLARE DEL TRATTAMENTO
- TRATTAMENTO CONTO TERZI
- Nuovi
- PRIVACY BY DESIGN PRIVACY BY DEFAULT
- ANALISI DEI RISCHI
  - Identificazione del rischio
  - Analisi del rischio
  - Trattamento del rischio
  - Minacce
  - Contromisure
  - Probabilità
  - Classificazioni incidenti
- ISO 27001
- EVIDENZE
- REGISTRO TRATTAMENTO
  - Censimento e analisi dei trattamenti effettuati dal titolare o responsabile
- DPIA PIA LIA
  - Valutazione d'impatto sulla protezione dei dati
- FORMAZIONE
  - Formazione privacy come misura di sicurezza obbligatoria
  - Piani di formazione diversificati in aula, e-learning, webinar
- BUSINESS CONTINUITY
  - Capacità di continuare a svolgere le proprie attività in seguito ad un incidente
  - DISASTER RECOVERY
  - BACKUP DATI
  - LINEA BACKUP
- DATA BREACH
  - Una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

E.S.G. (quando un'azienda può dirsi sostenibile: criteri di valutazione e impatti)
Rating della sostenibilità

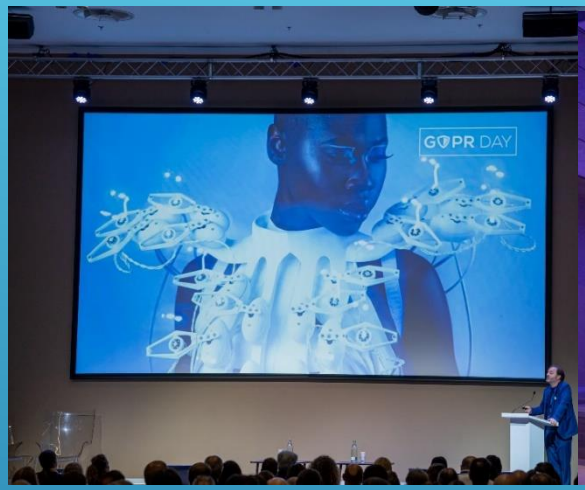
E. ENVIROMENT
S. SOCIAL
G. GOVERNANCE

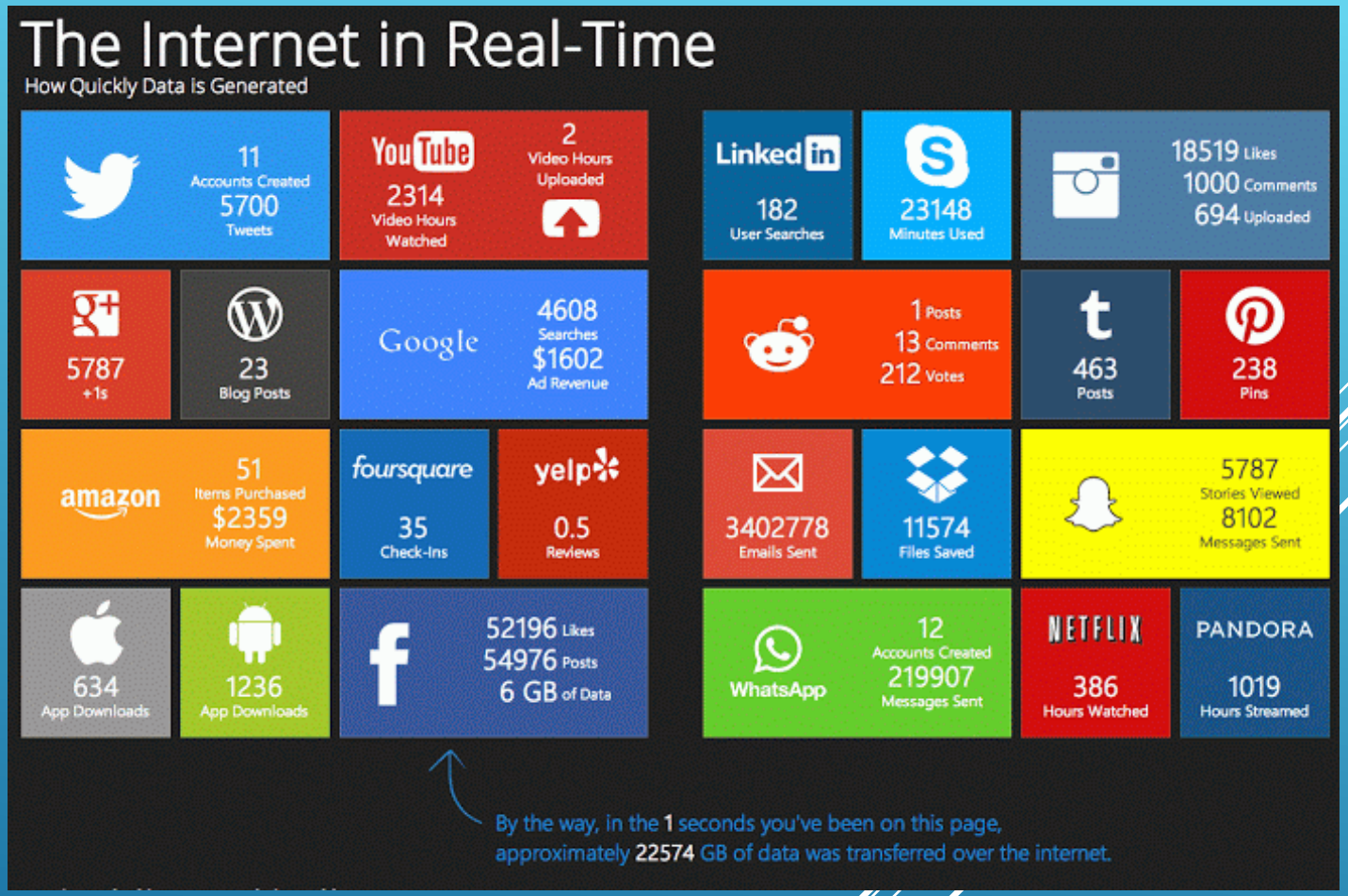
° Misure Ambientali (energia –rifiuti – CO_2)
° Misure di Sostenibilità (personale – turnover - sicurezza)
° Governance (Certificazioni – Etica – ISO – **Privacy dei Dati**)



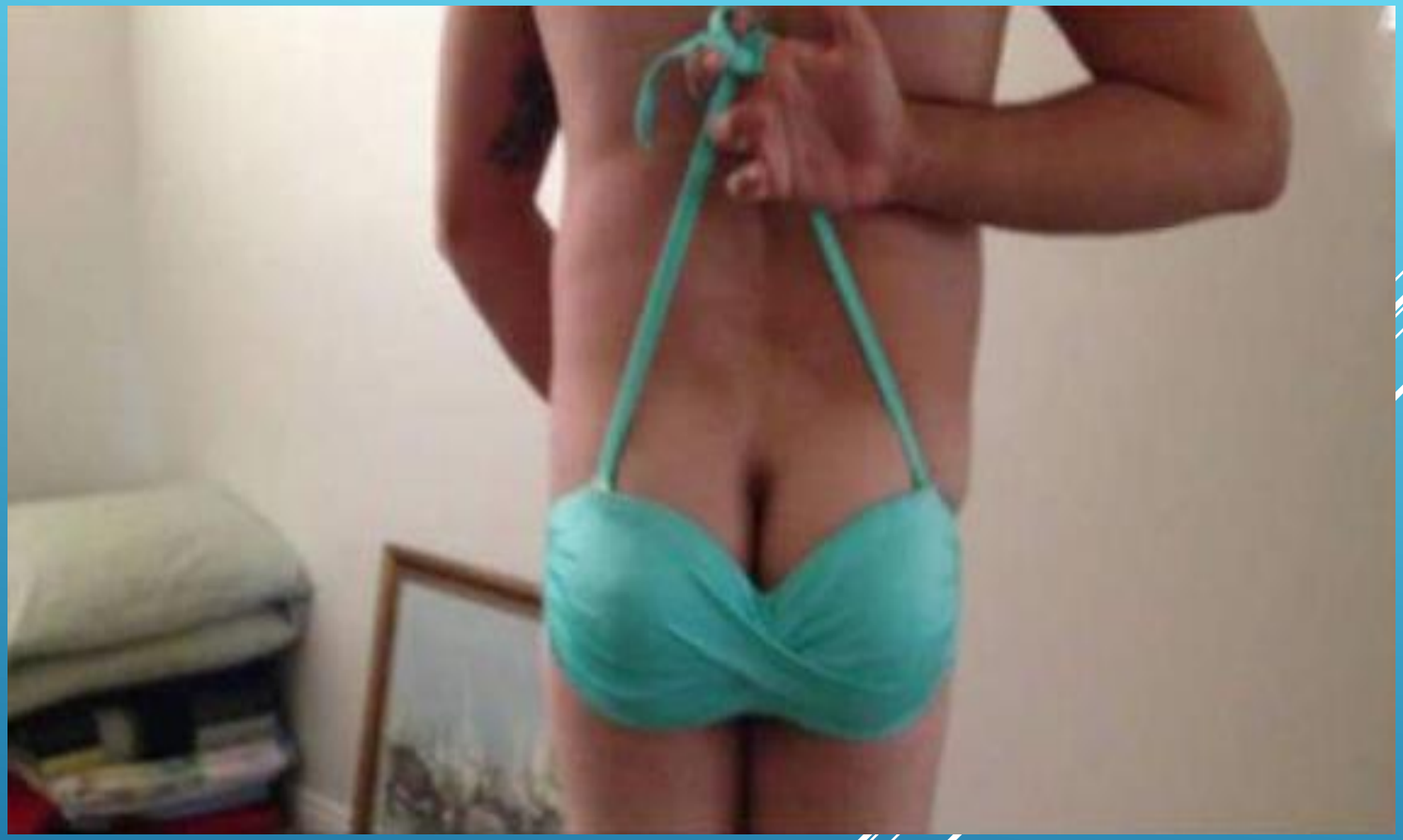
2024. Grandi imprese
2025. Società madri di grandi imprese
2026. ….
2028. Altre imprese

Contatto con il Garante e le Autorità





30 secondi : Fb 1.6 mil like 1.5 mil wa 6 mil tw 1.7 mil email 10 mil.



Potrebbero essere..?!

NICOLA
PAMELA

MARCO P.O.

Colossi della rete fb…
Google sa tutto di te ….non ci credi?

METEO IERI…DOMANI

Scandalo Facebook-Cambridge Analytica

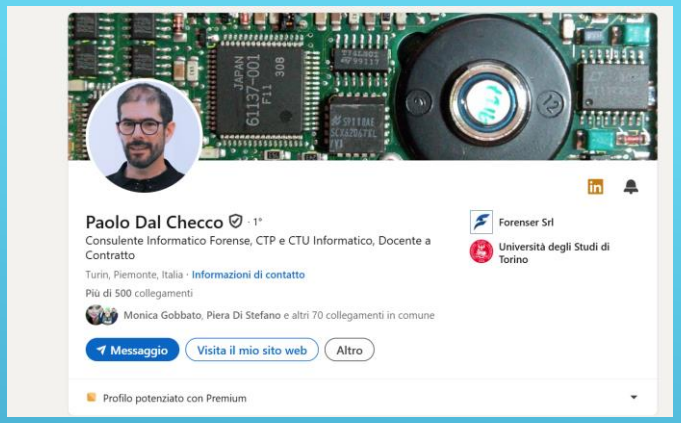
87 MIL DI UTENTI FACEBOOK UTILIZZANDO UN QUIZ This is your digital life

App ha raccolto dati anche degli amici degli utenti (moltiplicatore)
Like - informazioni personali - rete di amicizie
Comportamento on line -Dati demografici

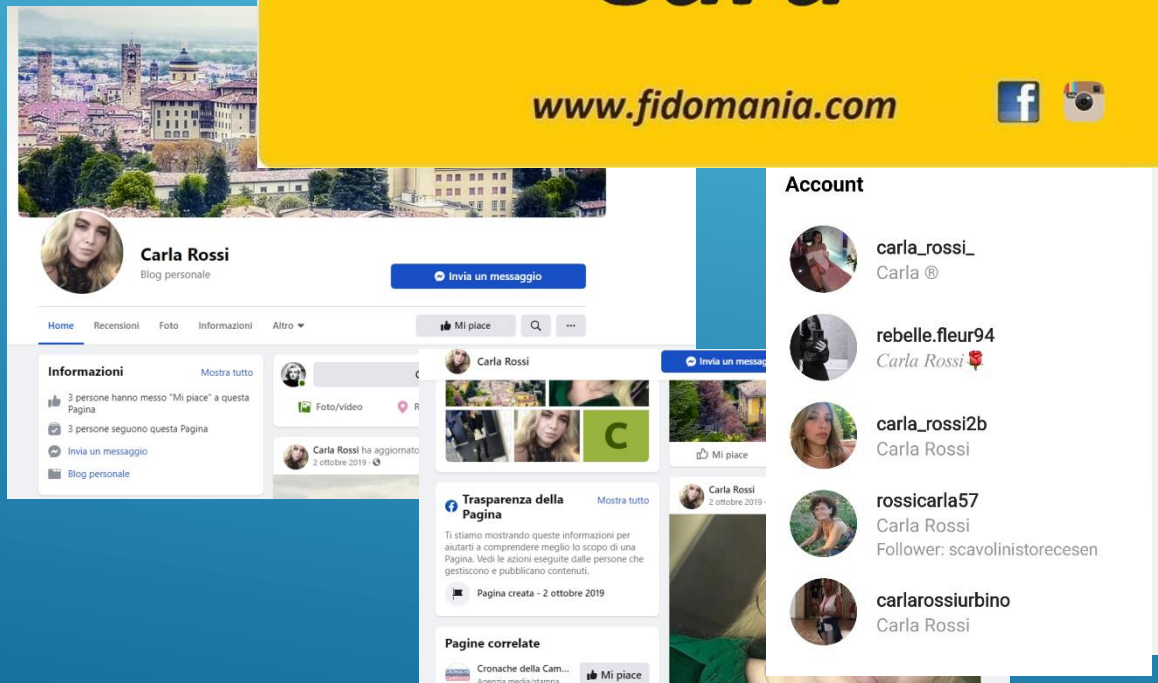
Sono stati usati per
Profili psicologici - Creare campagne politiche sulla Brexit

Lezioni apprese : sicuramente l'importanza del consenso
Valore commerciale dei dati

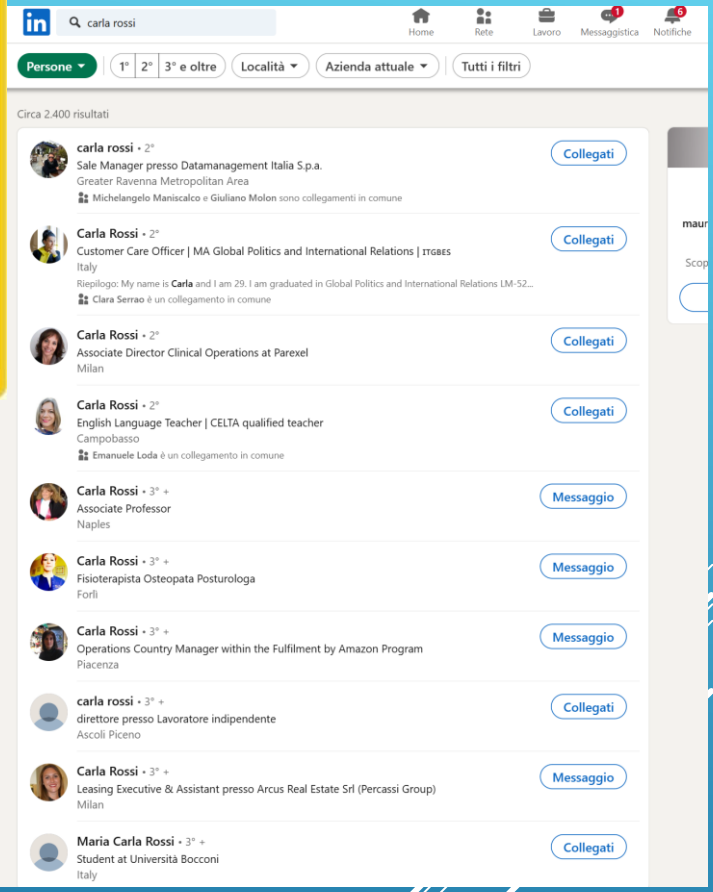
ESEMPI TRUFFE PAOLO DAL CHECCO




FIDOMania
TUTTO PER ANIMALI
Card
www.fidomania.com


Carla Rossi
Blog personale
Invia un messaggio
Home
Recensioni
Foto
Informazioni
Altro
Mi piace
Informazioni
Mostra tutto
3 persone hanno messo "Mi piace" a questa Pagina
3 persone seguono questa Pagina
Invia un messaggio
Blog personale
Foto/Video
Carla Rossi ha aggiornato
2 ottobre 2019
Carla Rossi
Trasparenza della Pagina
Mostra tutto
Ti stiamo mostrando queste informazioni per aiutarti a comprendere meglio lo scopo di una Pagina. Vedi le azioni eseguite dalle persone che gestiscono e pubblicano contenuti.
Pagina creata - 2 ottobre 2019
Pagine correlate
Cronache della Cam...
Agenzia media/stampa
Mi piace
Massiel Sanchez Sa...
Artista
Mi piace
Carla Rossi
Artista
Mi piace
Aggiungi la tua azienda su Facebook
Mostra il tuo lavoro, crea inserzioni e connettiti con clienti e sostenitori.
Mi piace
Commenta
Condividi

Account
carla_rossi_
Carla ®
rebelle.fleur94
Carla Rossi
carla_rossi2b
Carla Rossi
rossicarla57
Carla Rossi
Follower: scavolinistorecesen
carlarossiurbino
Carla Rossi


carla rossi
Home
Rete
Lavoro
Messaggistica
Notifiche
Persone
1°
2°
3° e oltre
Località
Azienda attuale
Tutti i filtri
Circa 2.400 risultati
carla rossi • 2°
Sale Manager presso Datamanagement Italia S.p.a.
Greater Ravenna Metropolitan Area
Michelangelo Maniscalco e Giuliano Molon sono collegamenti in comune
Collegati
Carla Rossi • 2°
Customer Care Officer | MA Global Politics and International Relations | ITGBES
Italy
Riepilogo: My name is Carla and I am 29. I am graduated in Global Politics and International Relations LM-52...
Clara Serrao è un collegamento in comune
Collegati
Carla Rossi • 2°
Associate Director Clinical Operations at Parexel
Milan
Collegati
Carla Rossi • 2°
English Language Teacher | CELTA qualified teacher
Campobasso
Emanuele Loda è un collegamento in comune
Collegati
Carla Rossi • 3° +
Associate Professor
Naples
Messaggio
Carla Rossi • 3° +
Fisioterapista Osteopata Posturologa
Forlì
Messaggio
Carla Rossi • 3° +
Operations Country Manager within the Fulfilment by Amazon Program
Piacenza
Messaggio
carla rossi • 3° +
direttore presso Lavoratore indipendente
Ascoli Piceno
Collegati
Carla Rossi • 3° +
Leasing Executive & Assistant presso Arcus Real Estate Srl (Percassi Group)
Milan
Messaggio
Maria Carla Rossi • 3° +
Student at Università Bocconi
Italy
Collegati

20% AL 30 % OGNI ANNO DATI PERSONALI SUL DARK WEB

°INDIRIZZI EMAIL
°INDIRIZZI POSTALI
°NUMERI DI TELEFONO

Combinazioni email e password (pishing malware violazioni dati)
Pishing …spam via email con allegati o form

INFORMATIVA - CONSENSO

5-11-24

Il Garante della Privacy dà 20 giorni di tempo a Banca Intesa per informare i clienti sulla violazione dei loro dati personali

Dal Garante per la Privacy — Martedì, 05 Novembre 2024 17:15

Intesa Sanpaolo Spa ha 20 giorni di tempo per informare i clienti coinvolti nella **violazione dei propri dati personali e bancari**, avvenuta attraverso accessi indebiti effettuati da un dipendente della Banca.

È quanto deciso dal Garante Privacy a seguito dei chiarimenti inviati dall'Istituto bancario in risposta alla richiesta di informazioni dell'Autorità.

L'Autorità ritiene infatti, diversamente da quanto valutato dalla Banca, che la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone coinvolte, tenuto conto della natura della violazione, delle categorie dei dati trattati, della gravità e delle conseguenze che ne potrebbero derivare (ad es., la divulgazione di notizie riguardanti lo stato patrimoniale, il danno reputazionale).

Il provvedimento si è reso necessario poiché nelle prime comunicazioni inviate dalla Banca al Garante non era stata adeguatamente messa in evidenza l'ampiezza della violazione, come invece è poi risultata sia dagli articoli di stampa sia dai riscontri dalla stessa forniti.

Il Garante, che si riserva di valutare l'adeguatezza delle misure di sicurezza adottate nell'ambito di un'istruttoria tuttora in corso, ha inoltre ingiunto alla Banca di trasmettere all'Autorità, entro trenta giorni, un riscontro adeguatamente documentato sulle iniziative intraprese al fine di dare piena attuazione a quanto prescritto.

Fonte: Garante Privacy

13-10-24

13-10-24

sky tg24 | ELEZIONI USA | MEDIORIENTE | L'APP DI SKY TG24 | PODCAST | SKY TG24 INSIDER | SPETTACOLO

CRONACA | News | Approfondimenti | Numeri Pandemia | Vite | Scuola | Basta

CRONACA

Inchiesta Bari, da Meloni alla Juve: tutti i conti spiati dal bancario

13 ott 2024 - 10:00

©Ansa

Introduzione

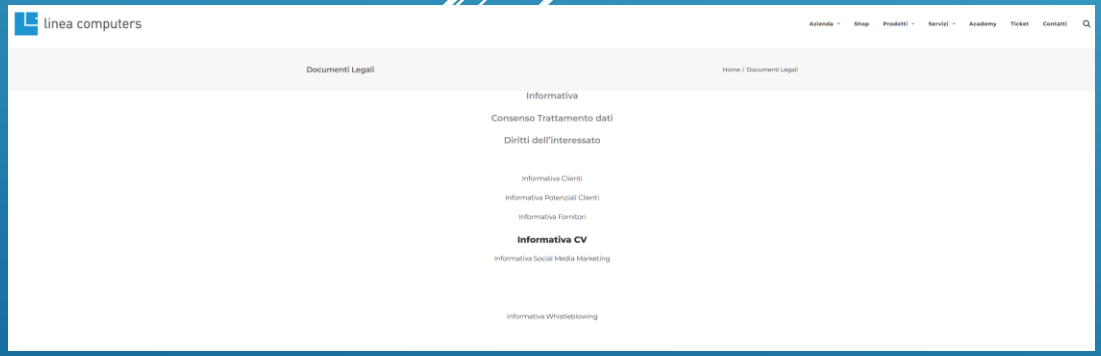
Con il passare dei giorni continuano a emergere nuovi nomi di politici, imprenditori, sportivi e altri personaggi pubblici i cui **conti correnti** e **carte di credito sono stati spiati** dall'ex dipendente di Intesa Sanpaolo della sede di Bisceglie (Bari), indagato dalla Procura del capoluogo pugliese per accesso abusivo ai sistemi informatici e tentato procacciamento di notizie concernenti la sicurezza dello Stato.

Tra i politici, spiccano i nomi della premier **Giorgia Meloni**, del presidente del Senato **Ignazio La Russa**, dei ministri **Matteo Salvini**, **Daniela Santanchè** e **Guido Crosetto**. Attenzionati anche ex premier come **Matteo Renzi**, **Mario Draghi**, **Massimo D'Alema** e **Silvio Berlusconi** (e figli). Non mancano poi sportivi come **Francesco Totti**, **Diego Armando Maradona** e la società **Juventus**. E poi ancora i cantanti **Al Bano**, **Antonello Venditti**, **Zucchero** e il presentatore televisivo **Paolo Bonolis**. Il 52enne ha anche controllato i conti di colleghi, concittadini, amici, parenti e conoscenti. Un totale di **6.600 accessi abusivi**.

TELECAMERE


ATTENZIONE
AREA SOTTOPOSTA A VIDEOSORVEGLIANZA
La registrazione è effettuata da:
LINEA COMPUTERS SRL
Dettagli del contatto responsabile della protezione dei dati:
gdpr@lineacomputers.com
Le immagini saranno conservate per un periodo di:
Le immagini registrate verranno conservate per il tempo necessario per le finalità per le quali sono acquisite.
Finalità della videosorveglianza:
Tutela del patrimonio aziendale.
È possibile accedere ai propri dati ed esercitare gli altri diritti riconosciuti dalla legge rivolgendosi a:
gdpr@lineacomputers.com
L'informativa completa sul trattamento dei dati è disponibile qui:


Linea Computers Srl
DATA PROTECTION POLICY


linea computers
Documenti Legali
Informativa
Consenso Trattamento dati
Diritti dell'interessato
Informativa Clienti
Informativa Potenziali Clienti
Informativa Fornitori
Informativa CV
Informativa Social Media Marketing
Informativa Whistleblowing

Protezione dei dati nell'UE

L'UE ha le norme più rigorose al mondo in materia di protezione dei dati. Nell'UE la protezione dei dati personali è considerata un diritto fondamentale.

Diritto di cancellazione ("diritto all'oblio") (art.17)

Il cosiddetto diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i titolari che hanno "reso pubblici" i dati personali dell'interessato, ad esempio pubblicandoli su un sito web, di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" *(art. 17, par. 2).*

Da sottolineare che l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (art. 17, par.1).

Diritto di cancellazione ("diritto all'oblio") (art.17)

Il cosiddetto diritto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali.

22 febbraio 2020 La Vis Pesaro 1898 riceve questa email
Silvia chiede

Inviato: sabato 22 febbraio 2020 15:55
A: segreteria@vispesaro1898.com
Oggetto: Art. 17 GDPR - Diritto alla cancellazione - Diritto all'oblio

Buongiorno, mi chiamo Marco Arcangeli (05/06/1993) ho giocato nella Vis Pesaro Juniores regionale fino al 2012.
In riferimento all'artico Art. 17 GDPR - Diritto alla cancellazione - Diritto all'oblio chiedo che i miei dati siano cancellati dal vostro data base e quindi non più sottoposti a trattamento dati personali perché non piu necessari per le finalità per le quali sono stati raccolti o trattati.

Grazie
In attesa
Marco Arcangeli

A quanto pare un ragazzo di 27 anni che chiede di essere "cancellato" ma onestamente non abbiamo nessun database! Parla di ultimo campionato nel 2012... nn ci sarà manco cartaceo!

Da: maurizio.sabattini@lineacomputers.com [mailto:maurizio.sabattini@lineacomputers.com]
Inviato: lunedì 24 febbraio 2020 12:53
A: 'Segreteria Vis Pesaro 1898' <segreteria@vispesaro1898.com>
Oggetto: R: Art. 17 GDPR - Diritto alla cancellazione - Diritto all'oblio

Azz chi è?
Vedo io e ti faccio sapere....potrebbe essere un caso da valutare nella riunione del 7/3
Maurizio

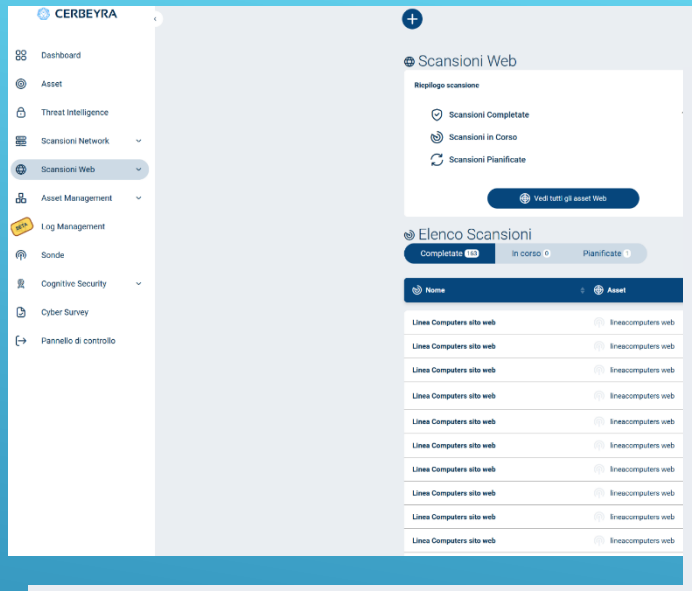
*
Comunque noi non abbiamo un data base dove memorizziamo i nostri giocatori
Parla del 2012, non abbiamo neanche più quei computers.

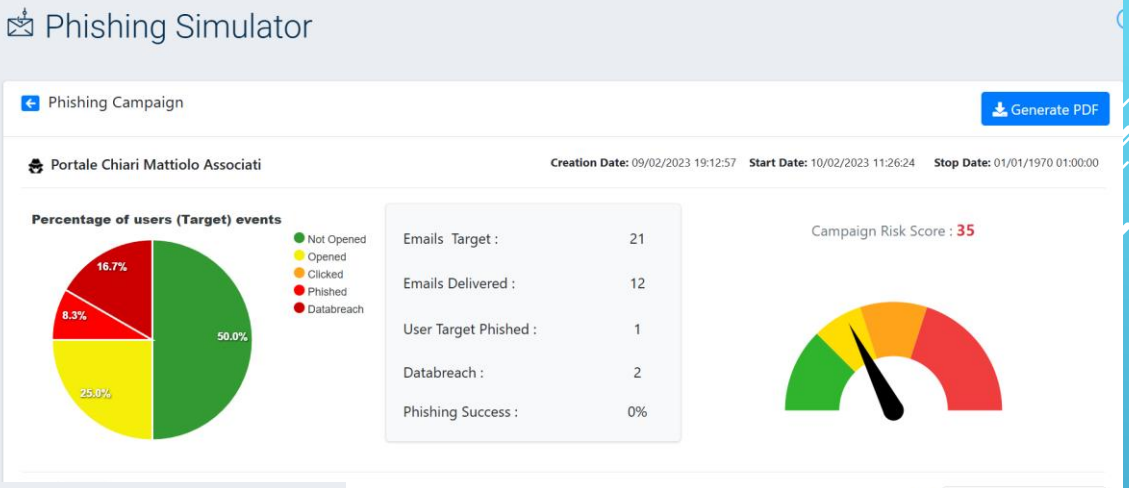
Sicuramente abbiamo a livello cartaceo il tesseramento ma quello è un problema della Lega non possiamo cancellare i dati in lega

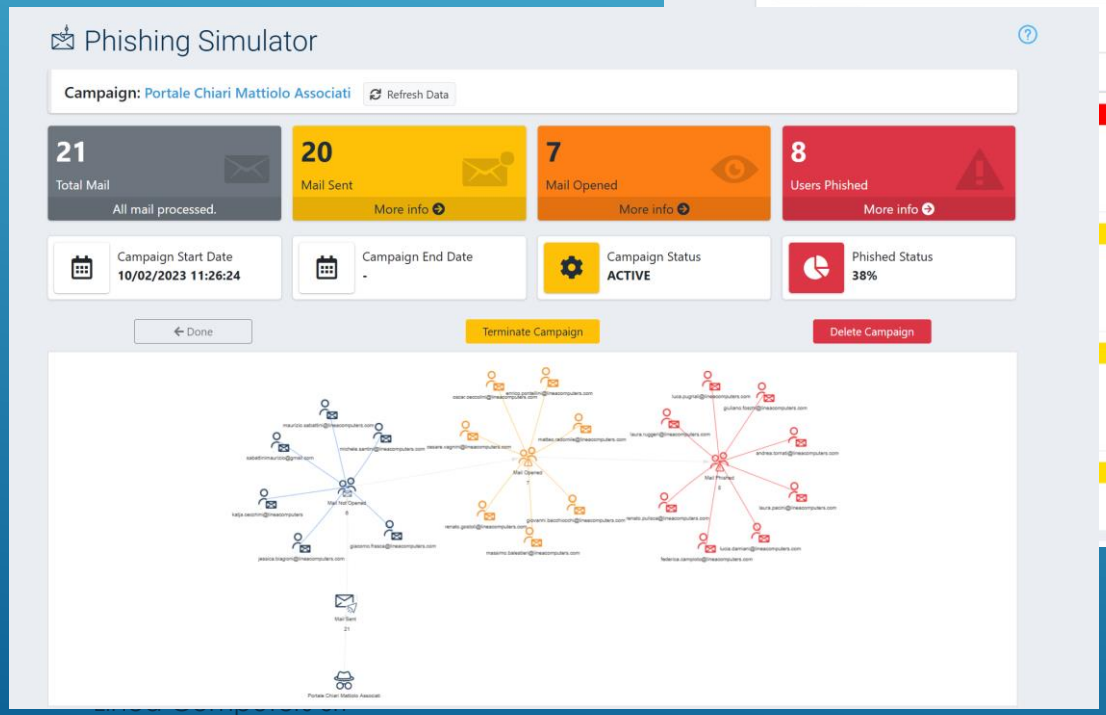
Dal momento della richiesta mi sembra di vedere 22 febbraio 15 55
Abbiamo un mese di tempo (22/3) per rispondere al giocatore
Dicendo che i suoi dati in nostro possesso sono stati cancellati dai nostri archivi e dai nostri backup tranne eventuali ricevute fiscali o altro documento fiscale che per quel trattamento deve rimanere a disposizione per 10 anni.
Grazie
maurizio

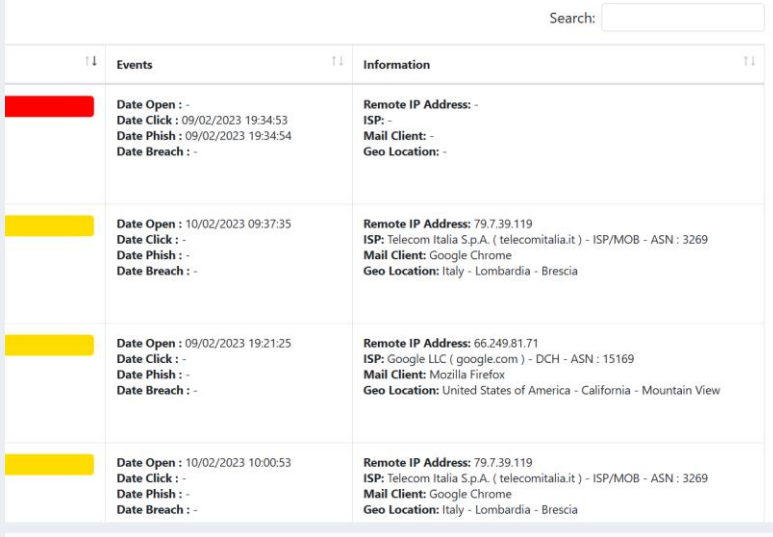
Da: Segreteria Vis Pesaro 1898 [mailto:segreteria@vispesaro1898.com]
Inviato: lunedì 24 febbraio 2020 12.15
A: maurizio.sabattini@lineacomputers.com
Oggetto: I: Art. 17 GDPR - Diritto alla cancellazione - Diritto all'oblio

Ho ricevuto questa mail.... Che dovremmo fare secondo te ?


CERBEYRA
Dashboard
Asset
Threat Intelligence
Scansioni Network
Scansioni Web
Asset Management
Log Management
Sonde
Cognitive Security
Cyber Survey
Pannello di controllo
Scansioni Web
Riepilogo scansione
Scansioni Completate
Scansioni in Corso
Scansioni Pianificate
Vedi tutti gli asset Web
Elenco Scansioni
Completate 183
In corso 0
Pianificate 1
Nome
Asset
Linea Computers sito web
lineacomputers web


Phishing Simulator
Phishing Campaign
Generate PDF
Portale Chiari Mattiolo Associati
Creation Date: 09/02/2023 19:12:57
Start Date: 10/02/2023 11:26:24
Stop Date: 01/01/1970 01:00:00
Percentage of users (Target) events
16.7%
8.3%
50.0%
25.0%
Not Opened
Opened
Clicked
Phished
Databreach
Emails Target : 21
Emails Delivered : 12
User Target Phished : 1
Databreach : 2
Phishing Success : 0%
Campaign Risk Score : 35


Phishing Simulator
Campaign: Portale Chiari Mattiolo Associati
Refresh Data
21
Total Mail
All mail processed.
20
Mail Sent
More info
7
Mail Opened
More info
8
Users Phished
More info
Campaign Start Date
10/02/2023 11:26:24
Campaign End Date
-
Campaign Status
ACTIVE
Phished Status
38%
Done
Terminate Campaign
Delete Campaign


Search:
Events
Information
Date Open : -
Date Click : 09/02/2023 19:34:53
Date Phish : 09/02/2023 19:34:54
Date Breach : -
Remote IP Address: -
ISP: -
Mail Client: -
Geo Location: -
Date Open : 10/02/2023 09:37:35
Date Click : -
Date Phish : -
Date Breach : -
Remote IP Address: 79.7.39.119
ISP: Telecom Italia S.p.A. (telecomitalia.it) - ISP/MOB - ASN : 3269
Mail Client: Google Chrome
Geo Location: Italy - Lombardia - Brescia
Date Open : 09/02/2023 19:21:25
Date Click : -
Date Phish : -
Date Breach : -
Remote IP Address: 66.249.81.71
ISP: Google LLC (google.com) - DCH - ASN : 15169
Mail Client: Mozilla Firefox
Geo Location: United States of America - California - Mountain View
Date Open : 10/02/2023 10:00:53
Date Click : -
Date Phish : -
Date Breach : -
Remote IP Address: 79.7.39.119
ISP: Telecom Italia S.p.A. (telecomitalia.it) - ISP/MOB - ASN : 3269
Mail Client: Google Chrome
Geo Location: Italy - Lombardia - Brescia

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case aplhabets	Mixed numbers, Lower and Upper case aplhabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

2014 Il capo della sicurezza dei mondiali di calcio rivela la password Wi-Fi ... Hanno fatto come quelli che "nascondono" la password nel post-it ...

RANSOMWARE

chiedono il pagamento
del riscatto in Bitcoin o altre criptovalute,
poiché queste valute digitali sono difficili da rintracciare.

Il funzionamento del ransomware consiste nel blocco dell'accesso ai file sul computer infetto, al quale segue la richiesta di un riscatto per ripristinare l'accesso ai dati.

Dati che spesso finiscono nel Dark Web

Costo del danno reputazionale: le conseguenze di un data breach sull'immagine di un'azienda

OGGI gli attuali algoritmi crittografici sono minacciati dalla potenza di calcolo dei computer quantistici. È quindi diventato necessario pensare allo sviluppo di nuovi algoritmi crittografici in grado di resistere al calcolo quantistico **Quantum-Safe Cryptography (QSC)**

23:26 59%

MULTA RECORD: IL GARANTE PRIVACY SANZIONA ENEL ENERGIA

4 Marzo 2024

Il Garante Privacy sanziona Enel Energia

La sanzione é frutto di un procedimento condotto dalla **Guardia di Finanza** nei confronti di quattro società che hanno trattato **dati personali** in modo illecito per finalità di **telemarketing**.

Già all'esito di questa prima fase l'**Autorità Garante** ha disposto la **confisca delle banche dati** utilizzate ed irrogato sanzioni pecuniarie dal valore complessivo di **un milione e 800mila euro**.

Nel corso di ulteriori accertamenti il Gar
ha potuto constatare che nella vicenda

Privacy - Termini

23:14 59%

ICO: tratta...
privacygdpr.it

ICO: trattamento dati biometrici lavoratori

23/02/2024 Sanzioni Garai

L'Information Commissioner's Off
ordinato (e sanzionato) a una soci
smettere di utilizzare la tecnologia
riconoscimento facciale (FRT) e la
delle impronte digitali per monitor
presenze dei dipendenti.

Il datore di lavoro non aveva fornit
dipendenti un'alternativa chiara all
scansione del volto e delle impron
per timbrare il cartellino di entrata
dal posto di lavoro.

Leggi la notizia sul sito dell'ICO

23:22 60%

No alla rilev...
privacygdpr.it

No alla rilevazione delle impronte digitali senza specifici requisiti

10/11/2022 Sanzioni Garanti Europei

Il Garante Privacy ha sanzionato per 20.000 euro una società sportiva che aveva introdotto un sistema di rilevazione delle impronte digitali per accertare la presenza dei dipendenti presso i club in gestione.

L'Autorità è intervenuta a seguito di una segnalazione di un'organizzazione sindacale, che lamentava l'introduzione del sistema biometrico da parte della società, nonostante la richiesta del sindacato di adottare me
azione meno invasivi.

Privacy - Termini

https://www.lineacomputers.com/mancato-riscontro-a-richiesta-daccesso-ai-dati-personali-sanzione/

*Il **tesserato** di una polisportiva **inviava un reclamo** al Garante in cui **sosteneva di aver ricevuto una email dalla polisportiva cui era tesserato dove erano indicati in chiaro tutti i destinatari** e per tale ragione aveva formulato una **richiesta di esercizio dei propri diritti di interessato** per poter accedere ai suoi dati personali trattati dalla polisportiva ed avere copia della relativa informativa privacy. Il reclamante proseguiva sostenendo di non aver mai ricevuto alcun riscontro.*

SANZIONE € 3.000 PER LA POLISPORTIVA

1. Gestione Email:
   - Uso corretto di CC e CCN
   - Come gestire allegati sensibili
   - Riconoscere email di phishing
   - Caso pratico: "Hai inviato per errore una lista clienti in CC anziché CCN"

2. Documenti cartacei:
   - Gestione delle stampe abbandonate
   - Smaltimento documenti sensibili
   - Policy "scrivania pulita"
   - Caso pratico: "Trovi un CV stampato alla stampante comune"

3. Password e Accessi:
   - Condivisione credenziali tra colleghi
   - Uso di dispositivi personali
   - Caso pratico: "Un collega ti chiede la password perché deve urgentemente accedere al tuo PC"

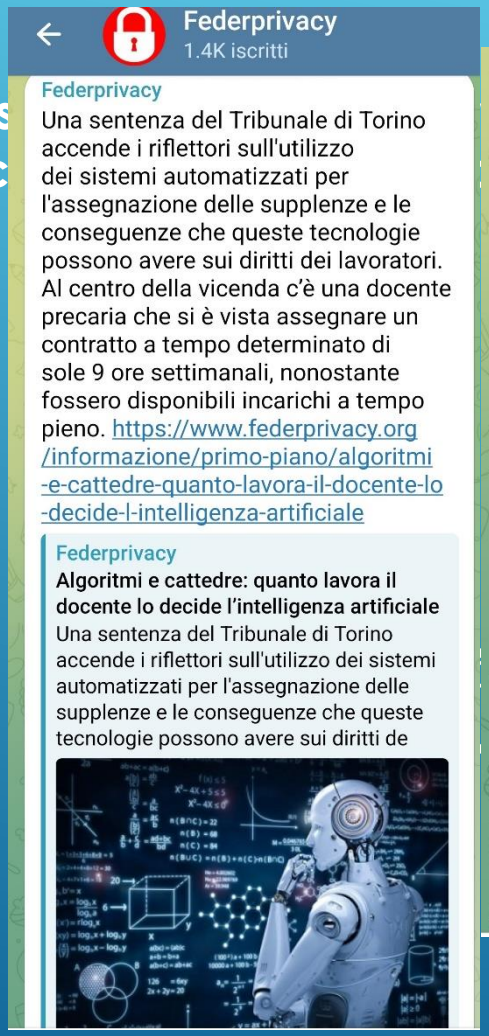
4. Richieste dei Clienti:
   - Verifica identità al telefono
   - Gestione richiesta dati via email
   - Diritto all'oblio
   - Caso pratico: "Un cliente chiede tutti i suoi dati personali via telefono"

5. Social Media:
   - Post di foto aziendali
   - Commenti su clienti/colleghi
   - Caso pratico: "Vuoi postare una foto del team building aziendale"

6. Visitatori in Ufficio:
   - Gestione badge
   - Accompagnamento ospiti
   - Caso pratico: "Un 'tecnico' si presenta in ufficio senza appuntamento"

20% AL 30 % OGNI ANNO DATI PERSONALI SUL DARK WEB

°INDIRIZZI EMAIL
°INDIRIZZI POSTALI
°NUMERI DI TELEFONO



Pishing cartaceo

Il postino vi porta il virus informatico

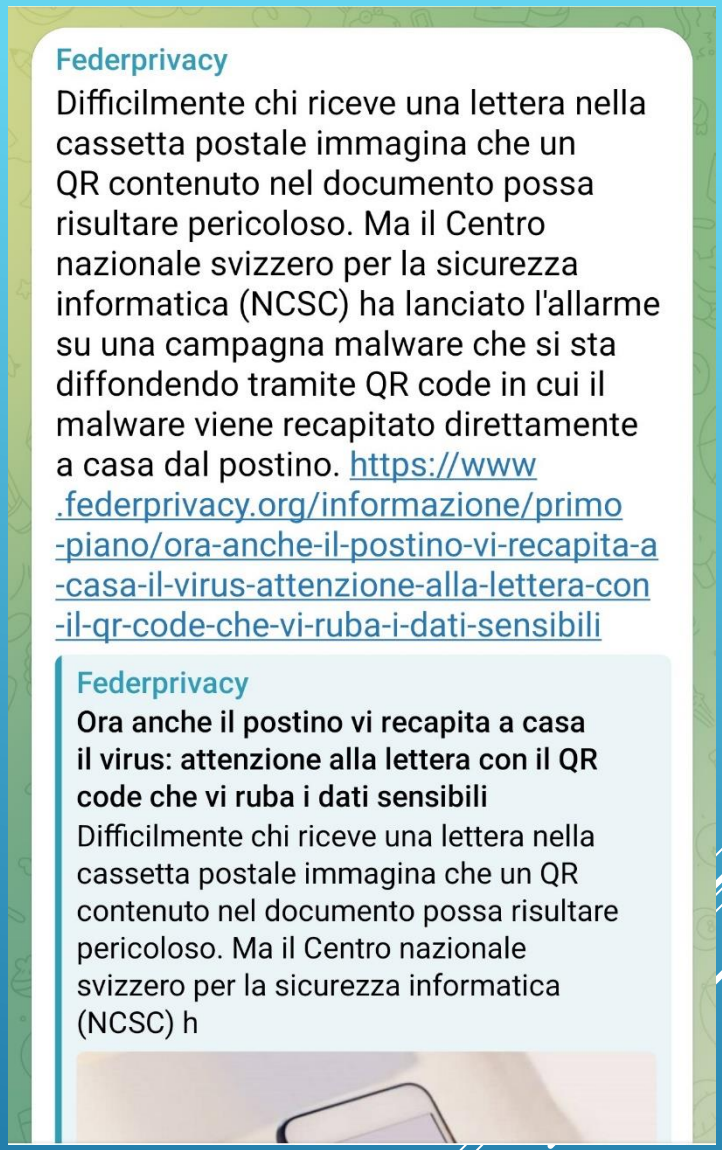
Ne è un esempio la campagna malware che si sta infatti diffondendo proprio tramite QR code sul territorio svizzero. Nulla di nuovo sotto il sole, se non fosse che i codici malevoli vengono recapitati direttamente a casa dal postino.

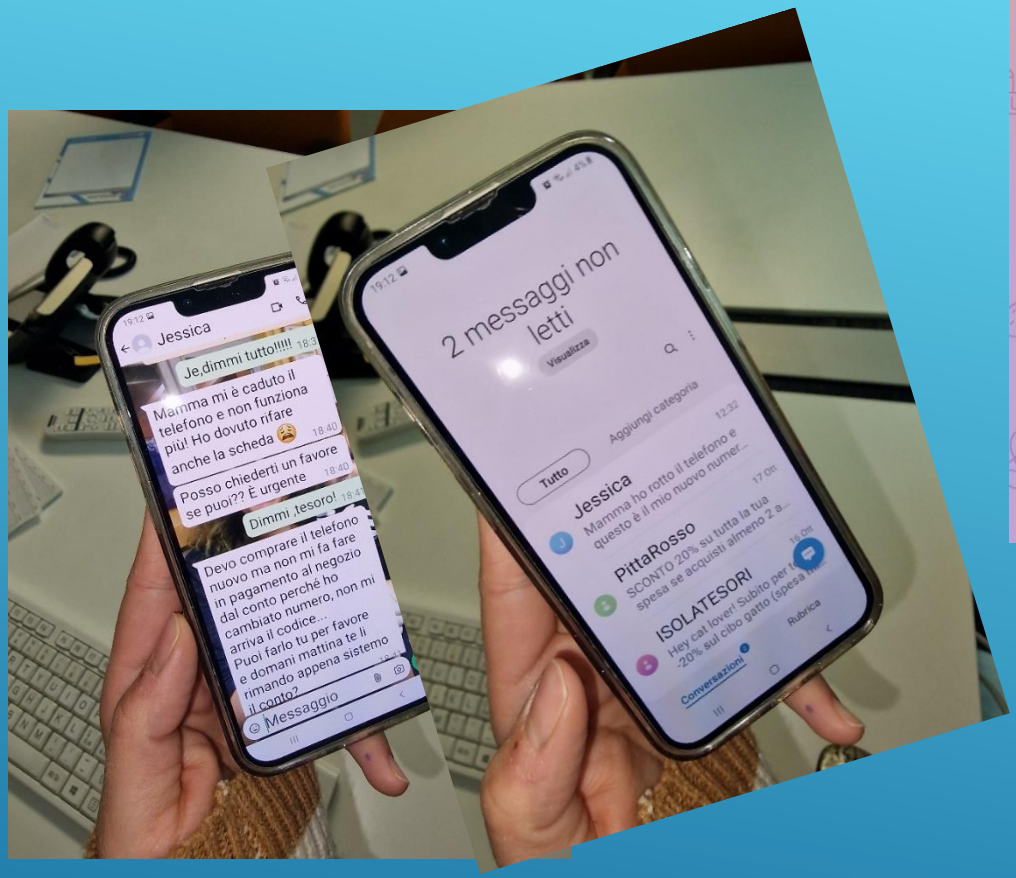
E dato che difficilmente chi riceve una lettera nella cassetta postale immagina che un QR contenuto nel documento possa risultare pericoloso, il Centro nazionale svizzero per la sicurezza informatica (NCSC) **non ha esitato a lanciare l'allarme** segnalando come diversi cittadini stanno ricevendo documenti apparentemente relativi all'Ufficio federale di meteorologia e climatologia, ma che in realtà hanno uno scopo fraudolento.

La lettera in questione contiene un codice QR per lo scaricamento dell'app meteo disponibile sul territorio elvetico e nota come "*Alertswiss*", ma una volta scaricata ad essere installata è un'altra app che si chiama "*Severe Weather Warning*", la quale contiene un virus molto pericoloso.

Dopo l'installazione, il malware va a scaricare e installare una variante del trojan "Coper" (noto anche come "*Octo2*"), che agisce intercettando messaggi di autenticazione a due fattori, rubando credenziali bancarie e attuando altre operazioni simili. Coper ha accesso a oltre 383 app per smartphone, agendo anche direzionando gli utenti su pagine web di phishing finalizzate al furto di dati personali.

Il NCSC spiega che identificare il codice QR può non essere semplice, visto che le lettere cartacee comunicano un messaggio utile per la comunità e sembrano del tutto credibili, con tanto di logo ufficiale dell'Ufficio federale di meteorologia. Come sottolineato dagli esperti, in realtà con un po' di attenzione è possibile scovare delle piccole anomalie per capire se il codice è falso o manipolato evitando in extremis di cadere nella trappola. Ad esempio, l'app Alertswiss falsa, presenta una maiuscola di troppo, risultando "*AlertSwiss*" e svelando la sua dubbia natura. Inoltre, come da consuetudine in questi casi, l'app viene diffusa attraverso un sito web di terze parti e non da Google Play Store, come avviene per l'app ufficiale.




Jessica
Je,dimmi tutto!!!!!
Mamma mi è caduto il telefono e non funziona più! Ho dovuto rifare anche la scheda
Posso chiederti un favore se puoi?? È urgente
Dimmi ,tesoro!
Devo comprare il telefono nuovo ma non mi fa fare in pagamento al negozio dal conto perché ho cambiato numero, non mi arriva il codice... Puoi farlo tu per favore e domani mattina te li rimando appena sistemo il conto?
Messaggio
2 messaggi non letti
Visualizza
Tutto
Aggiungi categoria
Jessica
Mamma ho rotto il telefono e questo è il mio nuovo numer...
PittaRosso
SCONTO 20% su tutta la tua spesa se acquisti almeno 2 a...
ISOLATESORI
Hey cat lover! Subito per t... -20% sul cibo gatto (spesa...
Conversazioni
Rubrica


Mamma ho perso il telefono,questo é un nuovo numero lo puoi salvare e scrivermi su whatsapp? https://wa.me/3445718474
WhatsApp.com
Share on WhatsApp
WhatsApp Messenger: More than 2 billion people in over 180 countries use WhatsApp to stay in touch with friends and family, anytime and anywhere. WhatsApp is free and offers simple,...
16:40

Linea Computers Srl

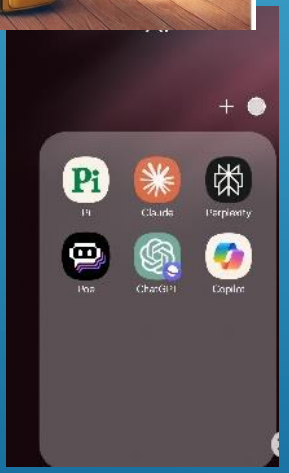
A.I. L'AI Act, la prima normativa a livello mondiale che stabilisce regole armonizzate sull'intelligenza artificiale, riserva uno spazio importante alla privacy e alla protezione dei dati personali, richiamando numerose volte il GDPR

Sorveglianza umana e decisioni automatizzate, profilazione, alla posizione geografica e al comportamento sui social media

La memoria di chat GPT.
Ecco cosa pensa GPT di **@maurizio_sabattini** di **@lineacomputers**.

.

L'art. 35 del GDPR disciplina la **valutazione d'impatto sulla protezione dei dati personali (DPIA)**, un adempimento fondamentale quando un trattamento può presentare un rischio elevato.



CV

L'APPROFONDIMENTO

Le aziende sono sempre più vulnerabili e proteggere il futuro digitale è ormai cruciale

Home > Attacchi Hacker E Malware: Le Ultime News In Tempo Reale E Gli Approfondimenti

L'intensa evoluzione digitale che stiamo vivendo ha portato enormi vantaggi nelle nostre vite, ma questa trasformazione, così rapida e dinamica, ci rende anche molto più vulnerabili perché spesso inconsapevoli o inesperti. E gli scenari che ci troviamo di fronte sono sempre più complessi

Pubblicato il 20 nov 2024

Stefania Prando
Business Development Manager di Kingston Technology

Obblighi	Soggetti Importanti
Audit e Supervisione Regolare	Non sottoposti a controlli regolari, solo in caso di sospetto.
Segnalazione degli Incidenti	Segnalazione entro 72 ore.
Sanzioni e Misure Correttive	Sanzioni fino a 7 milioni di euro o 1,4% del fatturato.
Supervisione delle Autorità	Supervisione meno invasiva, interventi su richiesta o in caso di incidenti.
Conformità agli Standard	Conformità agli standard internazionali non obbligatoria, solo raccomandata.
Responsabilità del Management	Meno responsabilità diretta per i dirigenti, sanzioni personali meno probabili.

LINEA COMPUTERS s.r.l.

Arriva la NIS 2

Di cosa parleremo?

- Cos'è la direttiva NIS 2
- Quali novità introduce
- A quali settori si applica
- Sanzioni previste per chi non si adegua
- Misure di sicurezza previste
- Scenari d'uso dell'autenticazione multi fattore

Obblighi per i soggetti interessati dalla NIS 2

Nella direttiva NIS2, molti **obblighi** si applicano sia ai **Soggetti Essenziali** che ai **Soggetti Importanti**, ma con alcune **differenze** in termini di **intensità, supervisione e requisiti specifici**.

OBBLIGHI PER ENTRAMBI I SOGGETTI (ESSENZIALI E IMPORTANTI)

Obblighi	Soggetti Essenziali	Soggetti Importanti
Valutazione e Gestione dei Rischi	Obbligatoria e costante, con una gestione più rigorosa e continua valutazione dei rischi cibernetici.	Obbligatoria, ma con requisiti meno stringenti per la frequenza delle valutazioni.
Misure di Sicurezza Tecniche e Organizzative	Devono adottare misure più rigorose (controllo degli accessi, crittografia, segmentazione della rete).	Devono adottare misure proporzionate, ma hanno maggiore flessibilità rispetto agli essenziali.
Monitoraggio e Segnalazione degli Incidenti	Devono notificare incidenti entro 24 ore dall'identificazione di un grave incidente.	Devono notificare incidenti entro 72 ore per incidenti rilevanti.
Piani di Continuità Operativa e Ripristino	Obbligo di sviluppare e aggiornare regolarmente piani di continuità e ripristino.	Obbligati a predisporre piani di continuità, ma con meno requisiti formali per aggiornamenti continui.
Formazione e Sensibilizzazione del Personale	Formazione obbligatoria e continua per tutto il personale.	Anche per loro la formazione è obbligatoria, ma con requisiti meno stringenti sulla frequenza.
Responsabilità del Management	I direttori e dirigenti sono direttamente responsabili e soggetti a sanzioni personali in caso di mancata conformità.	Anche qui il management è responsabile, ma la severità delle sanzioni è inferiore rispetto agli essenziali.
Collaborazione con le Autorità	Obbligo di cooperare attivamente con le autorità e partecipare a meccanismi di condivisione delle informazioni.	Devono collaborare, ma la supervisione delle autorità è meno invasiva.
Imposizione di Misure Correttive	Autorità competenti possono imporre misure correttive immediate e severe in caso di violazioni.	Le autorità possono imporre misure correttive, ma in modo meno stringente.
Conformità a Standard di Sicurezza Internazionali	Obbligatorio garantire la conformità a standard di sicurezza come ISO/IEC 27001.	Conformità incoraggiata, ma non obbligatoria in ogni caso.
Supervisione e Audit	Soggetti a controlli e audit regolari, sia interni che esterni, da parte delle autorità nazionali.	Soggetti a controlli meno frequenti e audit di intensità inferiore.
Sanzioni in caso di Inadempienza	Sanzioni più severe, fino a 10 milioni di euro o 2% del fatturato mondiale annuo.	Sanzioni più leggere, fino a 7 milioni di euro o 1,4% del fatturato mondiale annuo.
Segnalazione degli Incidenti	Devono segnalare incidenti entro 24 ore e fornire aggiornamenti continui sull'impatto e le azioni correttive.	Devono segnalare incidenti entro 72 ore, con meno requisiti per aggiornamenti continui.

Grazie.

ADESSO

Esame Live