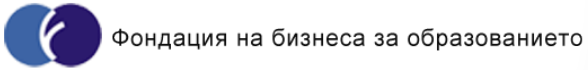
DiGiPort

Protecting personal data and privacy - GDPR

antic PAYS BASQUE

Co-funded by the Erasmus+ Programme of the European Union



Partnership

Co-funded by the
Erasmus+ Programme
of the European Union

Table of Contents

Co-funded by the
Erasmus+ Programme
of the European Union

Introduzione

Quando si è artisti in qualsiasi professione, a un certo punto ci si trova a raccogliere dati personali di clienti, futuri clienti, futuri collaboratori, ammiratori ecc.

Questi **dati personali** possono essere scritti in un quaderno come su un computer o possono essere raccolti automaticamente, ad esempio tramite moduli online, per esempio. Questo modulo di apprendimento fornisce una migliore comprensione su come proteggere i dati personali e la privacy negli ambienti digitali. Come utilizzare e condividere le informazioni di identificazione personale proteggendo se stessi e gli altri da eventuali danni. Utilizzare la "Privacy Policy" nei servizi digitali per informare su come vengono utilizzati i dati personali e quindi essere in conformità con il regolamento GDPR.

Co-funded by the
Erasmus+ Programme
of the European Union

Risultati dell'apprendimento

01

CAPIRE IL GDPR e i suoi concetti chiave
Evoluzione della protezione dei dati
Definizione di trattamento dei dati personali
A chi si applica il GDPR?

02

CONOSCERE I principi della protezione dei dati
Le otto regole d'oro per il trattamento, i dati, la sicurezza e la trasparenza: Finalità del trattamento - Conformità legale del trattamento - Minimizzazione dei dati - Protezione particolare di alcuni dati - Conservazione limitata dei dati - Obbligo di sicurezza - Trasparenza nei confronti degli stakeholder - Diritti delle persone sui propri dati

Co-funded by the Erasmus+ Programme of the European Union

Risultati dell'apprendimento

03

DEFINIRE le responsabilità degli attori
Nuova logica di accountability - Condivisione delle responsabilità - Responsabilità specifiche dei subappaltatori - Sanzioni e ricorsi

04

SET UP Il DPO e gli strumenti di compliance Il DPO e il registro dei dati - La notifica della violazione dei dati - La valutazione d'impatto sulla protezione dei dati - Codice di condotta e certificazione

Co-funded by the Erasmus+ Programme of the European Union

Teoria

DiGiPort

01

L'evoluzione della protezione dei dati: un po' di storia per capire meglio

1978

Gli inizi: in Francia, con la legge "Informatique et Libertés".

24 October 1995

Direttiva europea 95/46/CE adottata con i seguenti obiettivi
- la protezione delle persone e la libera circolazione dei dati
- fornire un quadro comune a tutti i Paesi dell'UE in termini di protezione dei dati personali - obbligo di adottare una legislazione per Paese + un organo di controllo indipendente

25 May 2018

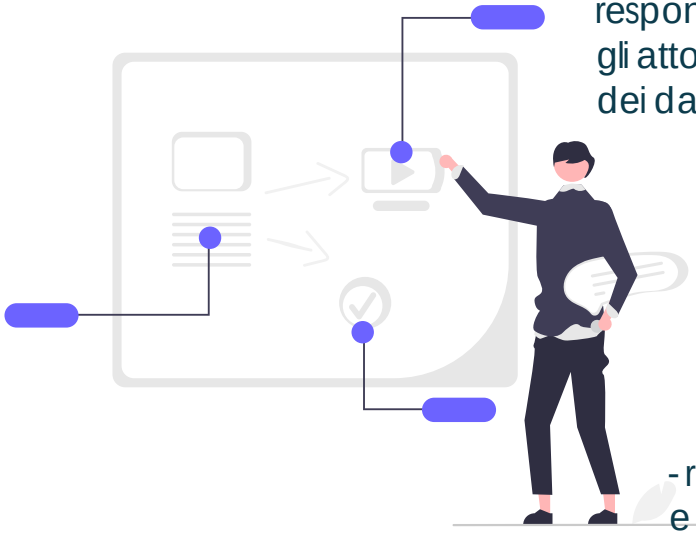
Un nuovo regolamento europeo che entra in vigore in ogni paese: il RGPD.

Co-funded by the Erasmus+ Programme of the European Union

> 3 principi fondamentali del GDPR

- una nuova logica di responsabilizzazione di tutti gli attori del trattamento dei dati

- il rafforzamento quantitativo e qualitativo degli individui

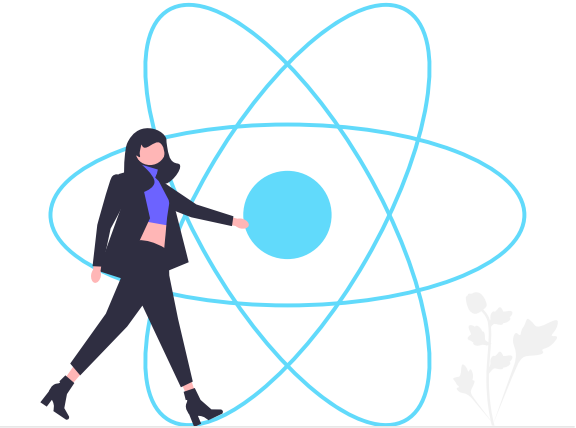


- rafforzamento del controllo e della sanzione delle strutture dedicate a livello nazionale

Co-funded by the Erasmus+ Programme of the European Union

Con lo sviluppo della dematerializzazione, degli oggetti connessi, degli algoritmi, il GDPR garantisce un adeguato livello di sicurezza delle informazioni trattate e offre alle persone la possibilità di comprendere e controllare meglio l'uso dei propri dati.

01



Lo sapevate?

- I dati personali sono alla base dello sviluppo dell'economia digitale.
- - I rischi legati all'utilizzo dei dati personali: "Il 95% dei possessori di smartphone può essere re-identificato incrociando almeno 4 delle loro posizioni geografiche (ad esempio i metadati delle foto)" Fonte: Arvind Narayanan che cita uno studio di YA de Montjoye - Unique in the Crowd: the privacy bounds of human mobility (Unico nella folla: i limiti della privacy della mobilità umana).

Co-funded by the Erasmus+ Programme of the European Union

01

Definizione del trattamento dei dati personali

I termini protezione e privacy dei dati sono spesso utilizzati in modo intercambiabile, ma esiste un'importante differenza tra i due.

La privacy dei dati definisce chi ha accesso ai dati, mentre la protezione dei dati fornisce strumenti e politiche per limitare effettivamente l'accesso ai dati. Le norme di conformità contribuiscono a garantire che le aziende soddisfino le richieste degli utenti in materia di privacy e sono responsabili dell'adozione di misure per la protezione dei dati privati degli utenti.

Personal data :

- dati indirettamente identificativi: numero di cliente associato a un nome

- dati direttamente identificativi: cognome, nome, foto, nome e-mail

- qualsiasi combinazione di informazioni in grado di identificare la persona: varie informazioni su un account di un social network, come ad esempio cosa vi piace, dove vivete o lavorate, ecc.

Co-funded by the Erasmus+ Programme of the European Union

"trattamento": qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati su dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la divulgazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Co-funded by the Erasmus+ Programme of the European Union

A chi si applica il GDPR?

Il GDPR si applica a tutte le organizzazioni pubbliche o private con sede nell'Unione Europea le cui attività sono rivolte a residenti europei. Questo vale sia che trattino i dati personali per conto proprio che in qualità di incaricati del trattamento.

Conclusione: se siete liberi professionisti, se trattate dati personali di cittadini europei e se la vostra azienda ha sede nell'UE, dovete rispettare le norme del RGPD!

Siete interessati se raccogliete per voi stessi i dati dei vostri potenziali clienti e clienti. Questo vale anche se siete coinvolti come fornitori di servizi in progetti che comportano il trattamento di dati personali (ad esempio, lo sviluppo di siti web).

Co-funded by the Erasmus+ Programme of the European Union

Responsabile e incaricato del trattamento dei dati

È importante capire che il GDPR non si applica allo svolgimento di attività strettamente personali come la rubrica di un telefono, il cloud con le foto di famiglia (eccezione domestica).

Tuttavia, il responsabile del trattamento dei dati è soggetto al GDPR, il cloud, l'operatore telefonico, il produttore dell'altoparlante collegato, ecc.

Co-funded by the Erasmus+ Programme of the European Union

Principi di protezione dei dati

8 regole d'oro riassunte in 4 buoni riflessi da adottare:

1- raccogliere solo i dati realmente necessari

2- essere trasparenti

3- pensare ai diritti delle persone

4- proteggere i dati

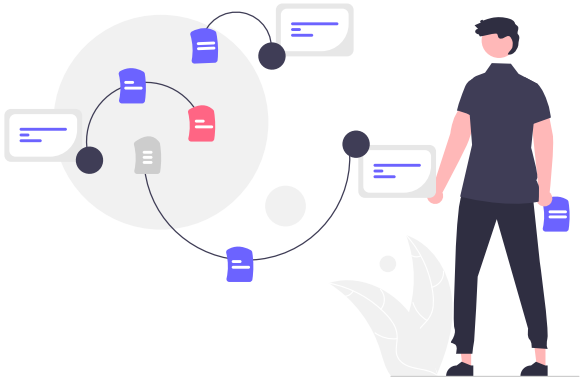
Base giuridica del trattamento: Un trattamento può essere effettuato solo se si basa su una delle 6 condizioni di conformità alla legge

Co-funded by the
Erasmus+ Programme
of the European Union

02

Principi di protezione dei dati: (vedi dettagli nell'allegato 1)

1- Finalità del trattamento: i dati personali raccolti possono essere trattati solo per una finalità precisa e legittima - La finalità definisce il legame tra i dati, le operazioni di trattamento e gli organismi che le attuano. La finalità definisce il legame tra i dati, le operazioni di trattamento e gli organismi che le realizzano. Definisce l'ambito del loro utilizzo.



2- Minimizzazione dei dati: Possono essere raccolti e trattati solo i dati strettamente necessari al raggiungimento dello scopo - I dati sono rilevanti se hanno un legame diretto con lo scopo del trattamento.

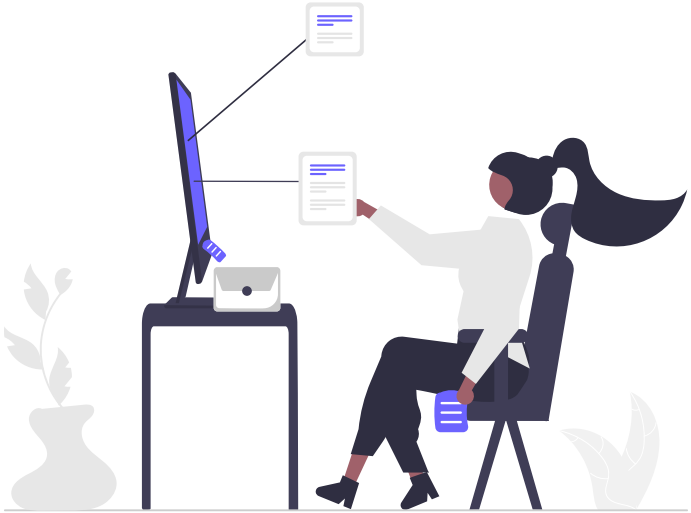
3- Protezione speciale dei dati sensibili: I dati sensibili possono essere raccolti e trattati solo a determinate condizioni.

Co-funded by the Erasmus+ Programme of the European Union

4- Conservazione limitata dei dati: I dati devono essere archiviati, cancellati o resi anonimi non appena viene raggiunto lo scopo per cui sono stati raccolti: - Obbligo di sicurezza (in considerazione dei rischi, devono essere attuate misure per garantire la sicurezza dei dati trattati).

5- Trasparenza: Le persone devono essere informate sull'uso dei loro dati e su come esercitare i loro diritti.

6- Diritti dell'individuo: Le persone hanno una serie di diritti che consentono loro di mantenere il controllo sui propri dati.



Co-funded by the
Erasmus+ Programme
of the European Union

Responsabilità degli attori

> Nuova logica di responsabilizzazione: in concreto, tutti gli attori coinvolti in un trattamento dovranno implementare e aggiornare le misure tecniche e organizzative per garantire in ogni momento il rispetto dei principi fondamentali del Regolamento.

- minimizzazione

- tempo di conservazione limitato

- sicurezza

- ecc.

Co-funded by the
Erasmus+ Programme
of the European Union

A seconda del contesto, devono nominare un responsabile della protezione dei dati, tenere un registro delle attività di trattamento, applicare una politica di riservatezza, effettuare una valutazione dell'impatto sulla privacy, ecc.

Gli strumenti obbligatori
- il registro delle attività di trattamento
- il responsabile della protezione dei dati
- in alcuni casi la valutazione d'impatto per determinati trattamenti
- la notifica delle violazioni dei dati a determinate condizioni.

Co-funded by the Erasmus+ Programme of the European Union

> condivisione delle responsabilità :

1/2 Qualora due o più responsabili del trattamento definiscano congiuntamente le finalità e i mezzi del trattamento, essi sono corresponsabili del trattamento. In questo caso, i contitolari del trattamento devono definire i rispettivi obblighi per contratto.

- Responsabilità specifiche dei subappaltatori: Le organizzazioni che trattano dati personali per conto dei loro clienti hanno responsabilità definite dal GDPR.

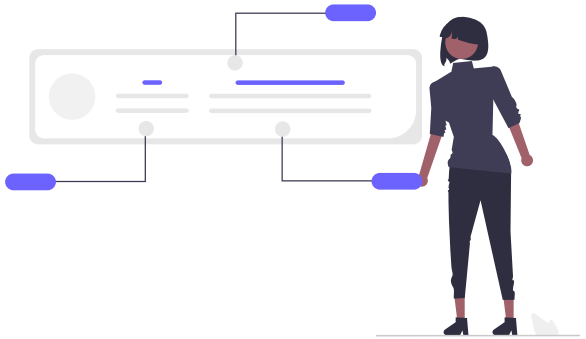
-> Fornitori di servizi IT (hosting, manutenzione ...)
-> Società di servizi digitali o ex società di servizi informatici e di ingegneria (SSII) che effettuano il trattamento dei dati...

Co-funded by the Erasmus+ Programme of the European Union

2/2

-> Società che offrono servizi di monitoraggio a distanza
-> Agenzie di marketing o di comunicazione che trattano dati personali per conto dei loro clienti
-> Fornitori di servizi di buste paga

I responsabili del trattamento, da parte loro, devono prestare attenzione alle condizioni in cui si rivolgono a un fornitore di servizi: la protezione degli interessati deve essere garantita lungo tutta la catena di esternalizzazione.



Co-funded by the
Erasmus+ Programme
of the European Union

> Sanzioni e ricorsi
RIMEDI: Reclami a un'autorità di controllo.

Chiunque ritenga che il trattamento dei dati personali che lo riguardano costituisca una violazione del GDPR può presentare un reclamo a un'autorità di controllo.

Questa può essere l'autorità dello Stato membro .
- dove l'individuo risiede abitualmente
- dove si trova il suo posto di lavoro
- dove si è verificata la violazione.

Co-funded by the
Erasmus+ Programme
of the European Union

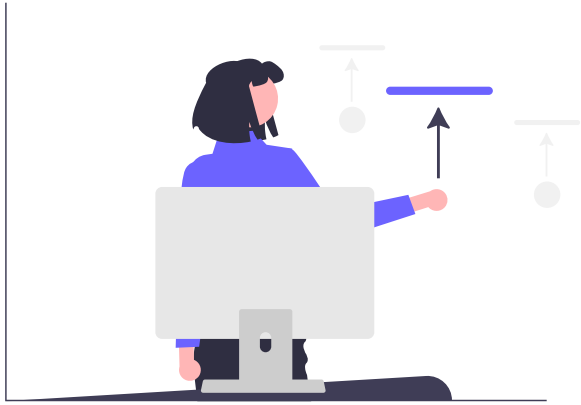
Graduazione delle sanzioni amministrative

L'importo massimo delle sanzioni amministrative differisce a seconda della gravità della violazione.

Il GDPR prevede all'articolo 83 che l'organismo indipendente del Paese possa decidere di imporre una multa fino a .

- 10 milioni di euro o 2% del fatturato mondiale

- 20 milioni di euro o il 4% del fatturato mondiale



Co-funded by the
Erasmus+ Programme
of the European Union

Il DPO e gli strumenti di compliance

> Il DPO - interno o esterno a tempo pieno o parziale - può essere condiviso. Deve essere formato, ma non è richiesta alcuna certificazione.

I suoi compiti .

1-Informare e consigliare l'organizzazione
2-Controllare la conformità
3-Fungere da interfaccia tra la propria organizzazione, l'organismo nazionale dedicato al GDPR e le persone interessate.

Il DPO è obbligatorio se si tratta di un servizio pubblico, di un'azienda privata che tratta molti dati personali o di un'organizzazione che tratta dati personali sensibili. Il DPO non è responsabile di eventuali violazioni.

Co-funded by the Erasmus+ Programme of the European Union

> Il registro dei dati

Ogni titolare o responsabile del trattamento deve istituire un registro delle attività di trattamento.
Si tratta di uno strumento essenziale nelle operazioni di compliance, che consente di identificare le attività di trattamento e, allo stesso tempo, di avere una visione d'insieme di ciò che viene fatto con i dati personali nelle organizzazioni.

Il GDPR richiede che il registro sia in forma scritta. Il suo formato è libero e può essere cartaceo o elettronico.

Co-funded by the Erasmus+ Programme of the European Union

Il registro è un documento di inventario e di analisi, che deve rispecchiare la realtà dei trattamenti e permettere di identificare con precisione

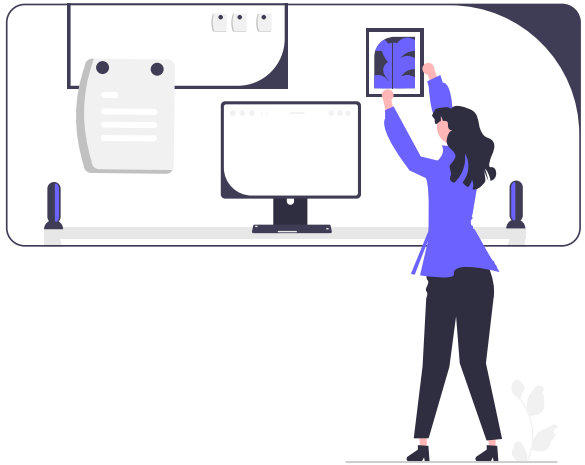
- i soggetti interessati (rappresentante, subappaltatore, contitolare del trattamento, ecc.) coinvolti nel trattamento dei dati

- le categorie di dati trattati l'utilizzo dei dati stessi

- chi accede ai dati e a chi vengono comunicati

- per quanto tempo vengono conservati i dati

- come vengono protetti



Co-funded by the
Erasmus+ Programme
of the European Union

Le aziende con meno di 250 dipendenti beneficiano di una deroga. Esse sono autorizzate a inserire nel registro solo le seguenti operazioni di trattamento:

- trattamenti ricorrenti (ad esempio, gestione delle buste paga, gestione di clienti, prospect e fornitori, ecc.)

- trattamenti che possono comportare un rischio per i diritti e le libertà delle persone (ad esempio, sistemi di geolocalizzazione, videosorveglianza, ecc.)

- trattamenti che coinvolgono dati sensibili (ad esempio, dati sanitari, reati, ecc.).

Co-funded by the Erasmus+ Programme of the European Union

Esempi di violazione dei dati:

- Un hacker accede al codice sorgente di un sito web e sovrascrive la visualizzazione del modulo di pagamento per recuperare le coordinate bancarie inserite, consentendo al contempo il pagamento, in modo che né l'utente né l'editore del sito web si accorgano del furto.

- Un'organizzazione specializzata nel trattamento di pazienti affetti da gravi patologie non riesce a effettuare il backup di oltre mille persone durante l'invio di un sondaggio.

Co-funded by the
Erasmus+ Programme
of the European Union

Termini di notifica

Se l'incidente costituisce un rischio per la privacy delle persone interessate, l'organizzazione deve notificare l'organismo competente nel paese in cui l'organizzazione è registrata

> Codice di condotta e certificazione

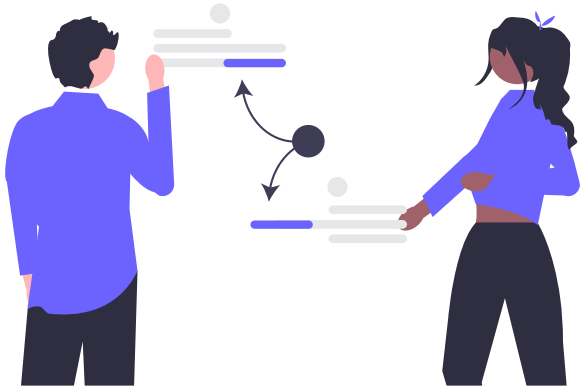
I codici di condotta e le certificazioni sono veicoli di conformità. Il GDPR richiede lo sviluppo di codici di condotta e/o schemi di certificazione per facilitare l'applicazione delle disposizioni del regolamento da parte di responsabili e incaricati del trattamento. Sono rivolti a tutti i professionisti, sia per le piccole che per le grandi aziende.

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

04

I codici di condotta sono un utile ausilio alla conformità per le organizzazioni, in quanto sono adattati al loro settore di attività. La certificazione di prodotti, processi, servizi e competenze dei delegati è un vantaggio significativo per un'organizzazione nei rapporti con i suoi partner o con le persone interessate dal trattamento dei dati in questione.



Co-funded by the Erasmus+ Programme of the European Union

Esempi e buone pratiche

https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/
Estratto di un articolo (FR) di uno specialista del RGPD

Jérôme de Mercey, cofondatore di Dastra ed ex agente CNIL, condivide i suoi consigli per le aziende.

(...) Quali sono i reparti più colpiti all'interno delle organizzazioni?
Il reparto vendite/marketing sarà in prima linea a causa dell'attività di prospezione commerciale, che può generare numerosi reclami da parte dei potenziali clienti, sempre più attenti all'uso dei dati. Il reparto Risorse Umane è storicamente molto colpito perché i dati trattati sono molto sensibili e spesso richiesti nell'ambito di controversie con i dipendenti.

Co-funded by the
Erasmus+ Programme
of the European Union

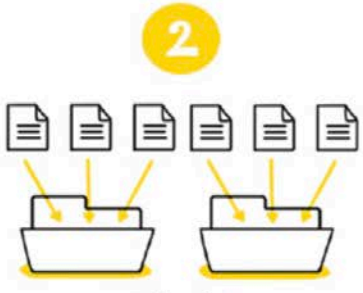
Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Esempi e buone pratiche

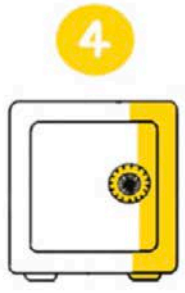
GDPR: agire in quattro mosse (Fonte: https://www.cnil.fr/fr/rgpd-par-ou-commencer)

Keep a register of your data processing



Sort out your data

Respect the rights individuals



Keep your data secure

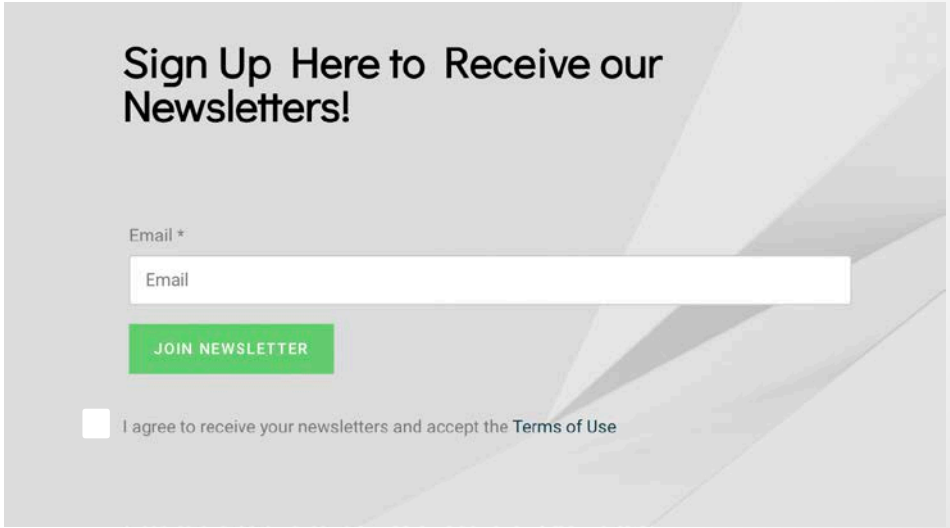
Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

Esempi e buone pratiche

Articolo con le migliori pratiche Politica di protezione dei dati: 9 cose fondamentali e 3 buone pratiche
https://cloudian.com/guides/data-protection/data-protection-policy-9-things-to-include-and-3-best-practices/

Un esempio - Sito web del progetto DIGIPORT
Inserire una casella di controllo per il consenso nei moduli di contatto o di iscrizione alla newsletter
–>>>>>



Esempi e buone pratiche

https://www.blogdumoderateur.com/conformite-rgpd-bonnes-pratiques/
Estratto da un altro articolo (FR) di uno specialista del RGPD

Jérôme de Mercey, cofondatore di Dastra ed ex agente CNIL, condivide i suoi consigli per le aziende.

(...) Come impostare una buona gestione dei cookie su un sito web? Quali sono i vostri consigli in questo campo? I cookie sono un argomento complesso perché non si limitano ai soli cookie. Bisogna anche vedere tutto ciò che passa attraverso la rete ed essere in grado di capire lo scopo e i destinatari di ogni richiesta. È quindi necessario chiedere ai "conoscitori": i team di sviluppo dei siti web e metterli alla prova su ciò che viene depositato, letto e richiesto durante la navigazione del sito. È quindi necessario tradurre questi comportamenti e qualificarli rispetto alle normative, impostare un banner per i cookie e chiedere il consenso degli utenti di Internet se ciò è giustificato. Il modo più semplice per farlo è utilizzare uno strumento specializzato o farsi consigliare su come implementare questo banner. Potete anche leggere le linee guida della CNIL sull'argomento, che sono molto esplicite. (...)

Co-funded by the
Erasmus+ Programme
of the European Union

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

Esempi e buone pratiche

12 buone pratiche

https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

1.Formalizzare l'impegno del management

Il primo passo fondamentale è la formalizzazione dell'impegno della direzione. Infatti, è l'amministratore delegato il responsabile del trattamento. Egli rappresenta quindi l'azienda in caso di azione legale, sia che si tratti di una PMI che di una grande impresa.

2.Comunicare il contenuto del RGPD

È quindi necessario diffondere le informazioni sul regolamento all'interno dell'azienda, in modo chiaro e comprensibile, per sensibilizzare i dipendenti.

Co-funded by the Erasmus+ Programme of the European Union

DiGiPort

Esempi e buone pratiche

12 Good Practices
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

3.Formare i dipendenti
Una volta completata la fase di comunicazione, l'azienda può procedere alla formazione dei propri dipendenti e all'aggiornamento dei vari documenti relativi al trattamento dei dati (contratti, documenti HR).

4.Tenere un registro delle operazioni di trattamento
L'azienda deve inoltre tenere un registro delle attività di trattamento, che è un obbligo per il responsabile del trattamento. In caso di trattamenti che richiedano un monitoraggio regolare o un trattamento di dati di grandi dimensioni, deve nominare un responsabile della protezione dei dati ("DPO"), con la possibilità di ricorrere a un DPO esterno, se necessario.

Esempi e buone pratiche

12 Buone pratiche
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

5. Effettuare valutazioni di impatto sulla privacy
L'azienda deve studiare l'impatto sulla privacy dei vari processi effettuati sui dati personali dei propri clienti e dipendenti.

6. Stabilire un piano di verifica del trattamento
L'azienda deve anche implementare un piano di verifica del trattamento per garantire che il trattamento rimanga all'interno del quadro autorizzato dalla normativa. È necessaria una particolare vigilanza per i trasferimenti di dati al di fuori dell'Unione Europea.

Co-funded by the Erasmus+ Programme of the European Union

Esempi e buone pratiche

DiGiPort

12 Buone pratiche
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

7.Consentire la segnalazione di violazioni
L'azienda deve predisporre una procedura che consenta a chiunque di segnalare le violazioni dei dati personali.

8.Vigilare sull'esercizio dei diritti
Le aziende devono prestare particolare attenzione al rispetto dei diritti delle persone di cui detengono i dati, siano essi clienti o dipendenti, come il diritto all'oblio.

9. Monitorare la conformità nel tempo
Le aziende devono monitorare nel tempo la loro politica generale di protezione dei dati.

Co-funded by the
Erasmus+ Programme
of the European Union

Esempi e buone pratiche

12 Buone pratiche
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

10.Verifica della conformità dei fornitori
È importante valutare la conformità dei fornitori di servizi strategici e dei subappaltatori, in particolare di quelli che hanno accesso ai dati aziendali. I contratti dovrebbero essere rivisti per includere un certo numero di menzioni obbligatorie, che delimitino gli usi autorizzati.

11.Integrare la "Privacy by design" nelle pratiche
A livello tecnico, è necessario prestare attenzione alla conformità al RGPD sin dalla progettazione di nuovi servizi applicativi, integrando il principio della "Privacy by design" nelle pratiche di sviluppo. Questo principio si applica anche nel caso in cui l'azienda si avvalga di applicazioni sviluppate da un fornitore di servizi o acquisti software di terzi: deve stabilire il prima possibile i dati raccolti, il trattamento, i tipi di destinatari e il periodo di conservazione.

Co-funded by the
Erasmus+ Programme
of the European Union

Esempi e buone pratiche

12 Buone pratiche
https://itsocial.fr/partenaires/oracle-partenaire/articles-oracle/12-bonnes-pratiques-se-conformer-rgpd/

12.Prevedere un piano di backup dei dati
È essenziale anche l'implementazione di un piano di backup dei dati, con misure di protezione adeguate per i dati personali. L'azienda è infatti tenuta a garantire una sicurezza informatica rafforzata, con l'obbligo, in caso di violazione della sicurezza, di informare la CNIL entro 72 ore e, in alcuni casi, le persone interessate. Per il momento, solo il 51% delle aziende ha segnalato incidenti negli ultimi dodici mesi, il che suggerisce che c'è una carenza in questo settore.

Co-funded by the
Erasmus+ Programme
of the European Union

Esempi e buone pratiche

GDPR – Email Marketing -(Fonte : https://www.cnil.fr/fr/rgpd-par-ou-commencer)

Quando si tratta di email marketing, è necessario adottare le seguenti best practice:
- Non utilizzare una casella pre-selezionata o un'altra opzione predefinita.
- Separare la dichiarazione di consenso dalle altre condizioni.
- Scrivete in modo diverso: sì, voglio essere informato.
- Dare la possibilità di scegliere se acconsentire a operazioni di trattamento indipendenti.
- Dimostrare che l'annullamento dell'iscrizione e l'esercizio dei vari diritti sono facili.
- Assicurarsi che il consenso dei minori sia ottenuto legalmente.
- Documentate il più possibile l'ottenimento del consenso (ad esempio, il double opt-in).

Co-funded by the Erasmus+ Programme of the European Union

Co-funded by the
Erasmus+ Programme
of the European Union

DiGiPort

Fonti

https://www.cnil.fr/fr/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie

https://www.cnil.fr/en/home

https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

https://globalprivacyassembly.org/

https://www.oecd.org/

https://www.coe.int/en/web/portal/home

Co-funded by the
Erasmus+ Programme
of the European Union

APPENDICE

APPENDICE 1 : Base giuridica del trattamento: Un trattamento può essere effettuato solo se si basa su una delle 6 condizioni di liceità (cfr. dettagli nell'allegato 1).

- Finalità del trattamento: i dati personali raccolti possono essere trattati solo per una finalità precisa e legittima - La finalità definisce il legame tra i dati, le operazioni di trattamento e gli organismi che le attuano. La finalità definisce il legame tra i dati, le operazioni di trattamento e gli organismi che le eseguono. Definisce l'ambito del loro utilizzo.
- Minimizzazione dei dati: Possono essere raccolti e trattati solo i dati strettamente necessari al raggiungimento della finalità - I dati sono rilevanti se hanno un legame diretto con la finalità del trattamento.
- Protezione speciale dei dati sensibili: I dati sensibili possono essere raccolti e trattati solo a determinate condizioni.

Co-funded by the
Erasmus+ Programme
of the European Union

APPENDICE

ALLEGATO 1 : Base giuridica del trattamento: Un trattamento può essere effettuato solo se si basa su una delle 6 condizioni di liceità.

- Conservazione limitata dei dati: I dati devono essere archiviati, cancellati o resi anonimi non appena è stato raggiunto lo scopo per cui sono stati raccolti:
- Obbligo di sicurezza (in considerazione dei rischi, devono essere attuate misure per garantire la sicurezza dei dati trattati).
- Trasparenza: Le persone devono essere informate sull'uso dei loro dati e su come esercitare i loro diritti.
- Diritti delle persone: Le persone hanno una serie di diritti che consentono loro di mantenere il controllo sui propri dati.

Teoria

APPENDICE 1

Minimizzazione dei dati (possono essere raccolti e trattati solo i dati strettamente necessari al raggiungimento dello scopo - I dati sono rilevanti se sono direttamente collegati allo scopo del trattamento
- Per verificare se state rispettando il principio di minimizzazione, ponetevi le domande giuste: Qual è il mio scopo? Quali dati sono essenziali per raggiungere questo scopo? per raggiungere questo scopo? Ho il diritto di raccogliere questi dati? Ho fatto una chiara distinzione tra dati obbligatori e facoltativi?

Protezione speciale dei dati sensibili (i dati sensibili possono essere raccolti e trattati solo a determinate condizioni - i dati sensibili sono quelli che rivelano o riguardano:
- l'origine razziale o etnica - le opinioni politiche - le convinzioni filosofiche o religiose - l'appartenenza sindacale - la salute (fisica o mentale) - la vita sessuale o l'orientamento sessuale - i dati genetici - i dati biometrici allo scopo di identificare in modo univoco una persona fisica).

Co-funded by the Erasmus+ Programme of the European Union

Teoria

DiGiPort

APPENDICE 1

Conservazione limitata dei dati (I dati devono essere archiviati, cancellati o resi anonimi non appena viene raggiunto lo scopo per cui sono stati raccolti - Le organizzazioni devono essere in grado di giustificare il ciclo di vita dei dati in loro possesso: esigenze corrispondenti alle diverse fasi, dati e periodo di conservazione conservati per ciascuna di esse).

Obbligo di sicurezza (in considerazione dei rischi, devono essere attuate misure per garantire la sicurezza dei dati trattati - UNA PASSWORD CONCRETA I Una buona password deve contenere 12 caratteri, di almeno 4 tipi diversi: minuscole, maiuscole, numeri e caratteri speciali. Può essere più corta se il vostro account è dotato di ulteriori funzioni di sicurezza!) - Trasparenza (le persone devono essere informate sull'uso dei loro dati e su come esercitare i loro diritti) - Diritti delle persone (le persone hanno una serie di diritti che consentono loro di mantenere il controllo dei loro dati).

Co-funded by the
Erasmus+ Programme
of the European Union

Teoria

DiGiPort

APPENDICE 1

Trasparenza (le persone devono essere informate sull'uso dei loro dati e su come esercitare i loro diritti) - Diritti delle persone (le persone hanno una serie di diritti che consentono loro di mantenere il controllo sui propri dati - La limitazione del trattamento può essere richiesta solo in una delle seguenti 4 situazioni.

-Quando la persona ha esercitato il suo diritto di rettifica.
Il diritto alla limitazione si applica mentre il responsabile del trattamento verifica l'esattezza dei dati personali in questione. dei dati personali in questione (ha 1 mese di tempo)

- Quando la persona ha esercitato il suo diritto di opposizione.
Il diritto alla limitazione si applica per il tempo necessario a determinare se i legittimi interessi del responsabile del trattamento prevalgono su quelli dell'interessato.

Co-funded by the
Erasmus+ Programme
of the European Union

Teoria

DiGiPort

APPENDICE 1

- quando i dati stanno per essere cancellati mentre sono ancora necessari all'interessato per l'accertamento, egli può esercitare pretese legali

- quando il trattamento è illecito ma l'interessato preferisce la limitazione piuttosto che la cancellazione dei dati. Il GDPR consente quindi ai responsabili del trattamento di non dare seguito a una richiesta).

Il GDPR mette in atto meccanismi per compensare la mancanza di protezione dei dati in alcuni Paesi terzi. L'obiettivo è garantire che la "bolla di protezione" segua i dati in ogni momento.

Co-funded by the Erasmus+ Programme of the European Union