ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Recenti evoluzioni normative in materia (linee guida e raccomandazioni) su:
data breach, Brexit, trasferimenti all'estero, clausole standard, Covid-19, conferenze on-line

Protezione dei dati personali: panoramica su recenti evoluzioni normative

Cesare De Santis

Roma 23/04/2021

Agenda

- Presentazione relatore
- Protezione dei dati personali: panoramica su recenti evoluzioni normative
- Bibliografia & sitografia
- Q&A

Agenda

- **Presentazione relatore**
- Protezione dei dati personali: panoramica su recenti evoluzioni normative
- Bibliografia & sitografia
- Q&A

Presentazione relatore

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa/Aeronautica) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl a socio unico, che opera principalmente sui temi della conformità normativa e della protezione dei dati personali. Tra i clienti di PRIMAe srl si annoverano associazioni bancarie, banche, finanziarie, rappresentanze italiane di compagnie di assicurazione e riassicurazione europee, società immobiliari, altre società di consulenza. Assicuriamo il servizio DPO a alcune banche.

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM, iscritto nel registro dei consulenti privacy di KHC (http://www.khc.it/)

Agenda

- Presentazione relatore
- Protezione dei dati personali: panoramica su recenti evoluzioni normative
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- **Protezione dei dati personali: panoramica su recenti evoluzioni normative**
- Q&A
- Bibliografia & sitografia

Data breach: le linee guida

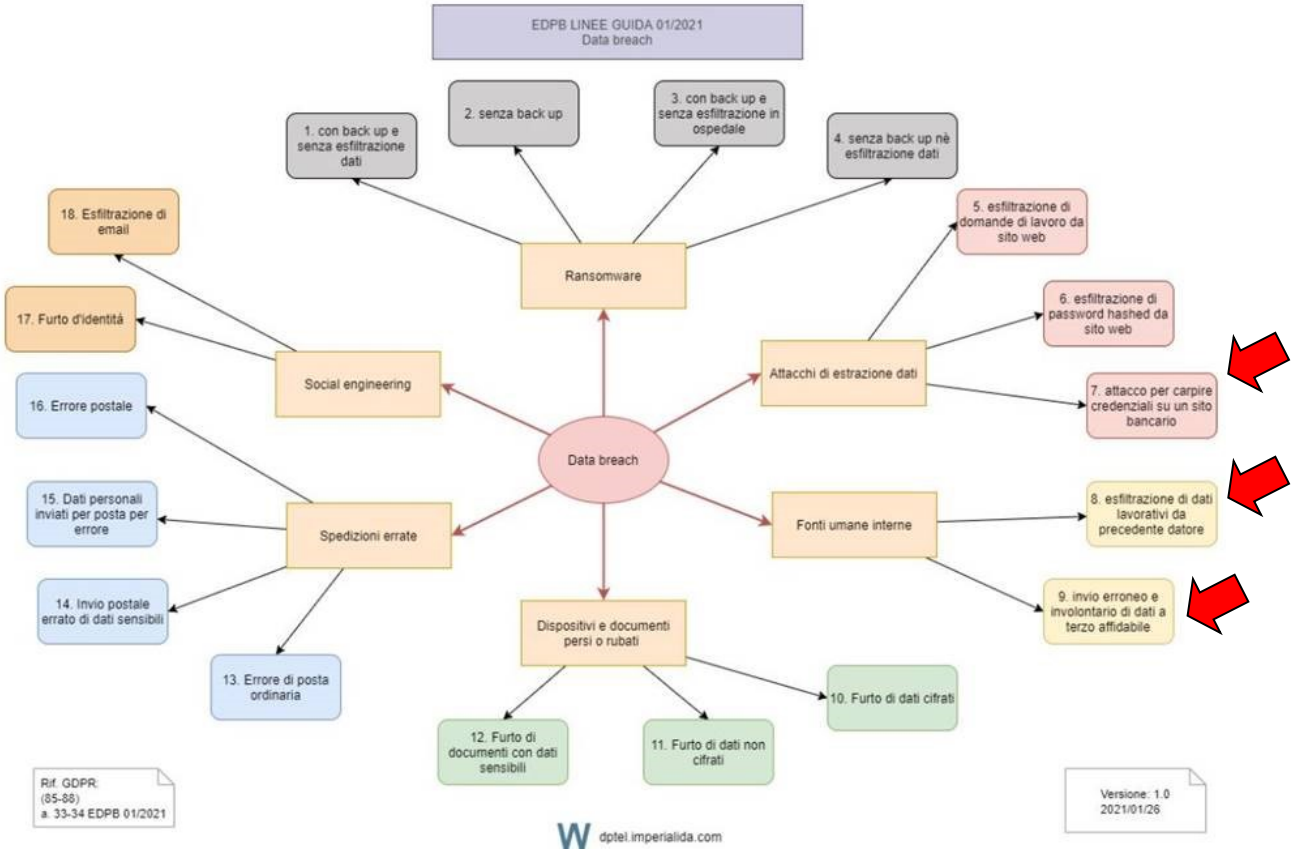
- «Violazione dei dati personali»: *la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati* (Art. 4 c. 12 e Considerando 85 GDPR).
- Nel GDPR è disciplinata da:
  - Art. 33 *«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 …omissis …»*
  - Art.34 *«**Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, **il titolare del trattamento comunica la violazione all'interessato** senza ingiustificato ritardo … omissis …»*
- Le linee guida di interesse sono:
  - Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 (WP250 febbraio 2018)
  - Recommendations for a methodology of the assessment of severity of personal data breaches (ENISA dicembre 2013)
  - Guidelines 01/2021 on Examples regarding Data Breach Notification (EDPB gennaio 2021)
- Per sapere se un indirizzo di posta elettronica o numero di telefono è stato coinvolto in un data breach si può accedere al link https://haveibeenpwned.com/ e digitarlo nella casella di ricerca.

Data Breach: gli esempi di EDPB

L'immagine sottostante è tratta dal sito "House of data" (https://houseofdataimperiali.com/2021/03/11/incidenti-da-fonti-umane-interne/) dell'avv. Rosario Imperiali

House of Data
IMPERIALI

Home Page Chi Siamo Servizi GDPR Academy Osservatorio Settori News



ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Data breach: il caso n. 7 di EDPB

Il caso descrive l'attacco al sito di una banca tramite la tecnica del c.d. "Credential stuffing"(1)

"A bank suffered a cyber-attack against one of its online banking websites. The attack aimed to enumerate all possible login user IDs using a fixed trivial password. The passwords consist of 8 digits. Due to a vulnerability of the website, in some cases information regarding data subjects (name, surname, gender, date and place of birth, fiscal code, user identification codes) were leaked to the attacker, even if the used password was not correct or the bank account not active anymore. This affected around 100.000 data subjects. Out of these, the attacker successfully logged into around 2.000 accounts which were using the trivial password tried by the attacker. After the fact, the controller was able to identify all illegitimate log-on attempts. The data controller could confirm that, according to antifraud checks, no transactions were performed by these accounts during the attack. The bank was aware of the data breach because its security operations centre detected a high number of login requests directed toward the website. In response, the controller disabled the possibility to log in to the website by switching it off and forced password resets of the compromised accounts. The controller communicated the breach only to the users with the compromised accounts, i.e. to users whose passwords were compromised or whose data was disclosed."

Gli obblighi individuati da EDPB in questo caso sono i seguenti:

68. Documenting the breach according to Article 33 (5) GDPR and notifying the SA about it are not optional in this scenario. Furthermore, the controller should notify all 100.000 data subjects (including the data subjects whose accounts were not compromised) in accordance with Article 34 GDPR.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	✓

(1) L'attacco consiste nel tentare accessi ripetuti ad un servizio web (portale, Facebook, ecc.) ad opera di un software malevolo (di seguito "bot") adoperando credenziali di accesso (username e password) precedentemente carpite attraverso una violazione di dati personali .Di fatto, si tratta di una variante del più noto attacco brute force che consiste nel tentare ripetutamente l'accesso con password inventate: la variante sta nel fatto che in questo caso si parte dalla conoscenza di almeno una credenziale valida, anche se per altri siti, e da questa si prova l'accesso direttamente e/o con varianti della medesima, riducendo i tempi normalmente necessari a trovare una password senza alcun riferimento." (dall'articolo "Credential stuffing e mancato contrasto al furto dati online: la CNIL sanziona i gestori di un sito Web" consultabile qui https://www.cybersecurity360.it/legal/privacy-dati-personali/credential-stuffing-e-mancato-contrasto-al-furto-dati-online-la-cnil-sanziona-i-gestori-di-un-sito-web/

Data breach: il caso n. 8 di EDPB

Il caso descrive la sottrazione di dati personali ad un'azienda da parte di un dipendente per fini privati

"During his period of notice, the employee of a company copies business data from the company's database he is authorized to access, and needs to fulfil his job. Months later, after quitting the job, he uses the data thus gained (mainly basic contact data) to contact the clients of the company to entice them to his new business

Gli obblighi individuati da EDPB in questo caso sono i seguenti:

77. All in all, as the given breach will not result in a high risk to the rights and freedoms of natural persons, a notification to the SA will suffice. However, the information to the data subjects might be beneficial for the data controller too, since it might be better that they hear from the company about the data leak rather than from the ex-employee who tries to contact them. Data breach documentation in accordance with Article 33 (5) is a legal obligation.

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	✓	X

Data breach : il caso n. 9 di EDPB

Il caso descrive l'invio di email ad un agente assicurativo (terzo fidato) contenente dati personali non facenti parte del suo ambito di competenza.

"An insurance agent noticed that – made possible by the faulty settings of an Excel file received by e-mail – he was able to access information related to two dozen customers not belonging to his scope. He is bound by professional secrecy and was the sole recipient of the e-mail. The arrangement between the data controller and the insurance agent obliges the agent to signal a personal data breach without undue delay to the data controller. Therefore, the agent instantly signalled the mistake to the controller, who corrected the file and sent it out again, asking the agent to delete the former message. According to the above-mentioned arrangement the agent has to confirm the deletion in a written statement, which he did. The information gained includes no special categories of personal data, only contact data and data about the insurance itself (insurance type, amount). After analysing the personal data affected by the breach the data controller did not identify any special characteristics on the side of the individuals or the data controller that may affect the level of impact of the data breach"

Gli obblighi individuati da EDPB in questo caso sono i seguenti:

Actions necessary based on the identified risks		
Internal documentation	Notification to SA	Communication to data subjects
✓	X	X

Tra le misure consigliate da EDPB:

*"**Periodic implementation of training, education and awareness programs for employees on their privacy and security obligations and the detection and reporting of threats to the security of personal data**. Develop an awareness program to remind employees of the most commons errors leading to personal data breaches and how to avoid them.»*

Data breach : il nuovo servizio del Garante privacy italiano

Il Garante privacy ha pubblicato un nuovo servizio online finalizzato a semplificare gli adempimenti di Titolari/Responsabili del trattamento in caso di *data breach.* In particolare si potrà accedere ad un questionario di *self-assessment* composto di cinque domande …

- ✓ **Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità di dati?**
- ✓ **L'incidente di sicurezza ha coinvolto dati personali?**
- ✓ **Sei titolare o responsabile del trattamento dei dati personali oggetto di violazione?**
- ✓ **È probabile che la violazione presenti un rischio per i diritti e le libertà degli interessati?**
- ✓ **La violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche?**

… rispondendo alle quali si avranno a disposizione le informazioni utili a intraprendere le azioni necessarie richieste dai diversi scenari di rischio. Precisiamo che l'Autorità, nelle informazioni rese relativamente alla risposta alla quarta domanda ed in relazione alle modalità di valutazione della gravità di una violazione, ha fatto riferimento alla metodologia indicata da ENISA (European Union Agency for Cybersecurity).

Data breach : la metodologia ENISA su gravità violazione (1)

Secondo ENISA i tre criteri fondanti il processo di valutazione della gravità di una violazione dei dati sono i seguenti:

- ✓ **contesto del trattamento** dei dati ove si verifica la violazione **(DPC)**: prende in considerazione il tipo di dati violati, congiuntamente ad altri fattori connessi all'ambito generale del trattamento;
- ✓ **facilità di identificazione (EI)**: determina la facilità con la quale si può individuare l'identità del soggetto interessato, grazie all'utilizzo dei dati coinvolti nella violazione;
- ✓ **circostanze della violazione (CB)**: analizza le specifiche circostanze connesse alla violazione presa esame (perdita di riservatezza dei dati, perdita di integrità, sussistenza di un comportamento doloso. etc.).

L'approccio della metodologia è il seguente:

- ✓ il **DPC** costituisce il fulcro dell'intero processo valutativo e stima la criticità dei dati in relazione ad uno specifico contesto di trattamento;

- ✓ l'**EI** è essenzialmente un fattore di correzione del DPC. Il livello di criticità complessiva di un trattamento di dati può essere ridotto in base al valore dell'EI. Minore è la facilità di identificazione conseguente alla violazione, infatti, minore è l'impatto complessivo della violazione stessa. Dalla combinazione di DPC ed EI (specificamente, dal prodotto dei loro valori) si ottiene il punteggio iniziale della gravità della violazione;

- ✓ il **CB** valuta specifiche circostanze (aggravanti) connesse alla violazione presa esame, che possono, a seconda dei casi, essere presenti o meno (perdita di riservatezza, integrità, disponibilità e comportamenti dolosi) . Per questa ragione, il coefficiente CB, quando presente, può solo contribuire ad aggravare la valutazione complessiva della violazione, sommandosi al punteggio iniziale, e ne valuta il loro potenziale effetto aggravante.

Data breach : la metodologia ENISA su gravità violazione (2)

Il punteggio complessivo attribuibile alla gravità di una violazione sarà, quindi, determinato dalla seguente formula:

SE = DPC * EI + CB

Il punteggio finale (SE) rappresenta il livello di gravità di una determinata violazione, considerando l'impatto che la stessa ha sui soggetti interessati i cui dati sono stati coinvolti nella violazione.

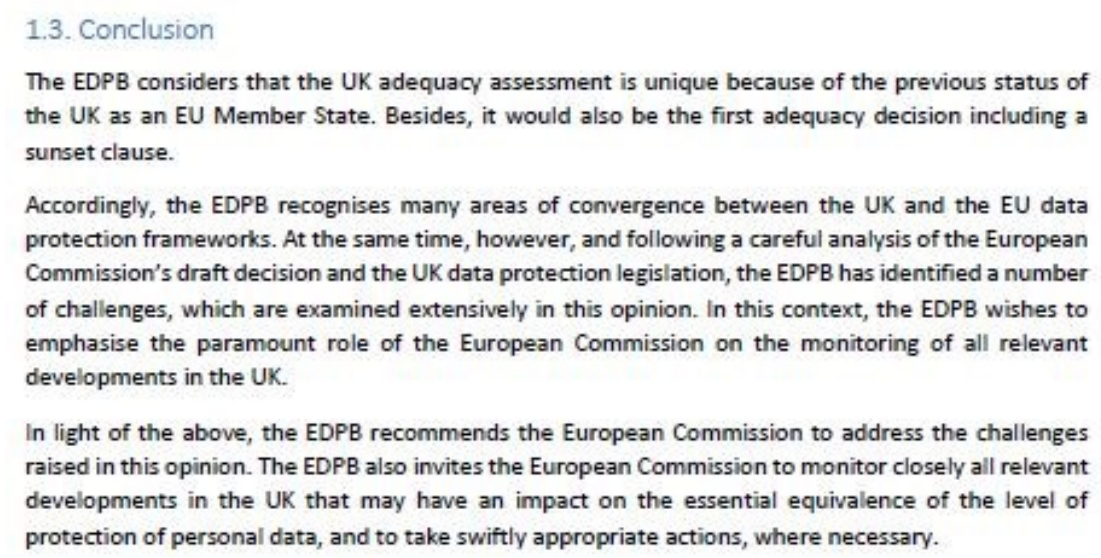
Gravità di una violazione di dati		
SE < 2	**Bassa**	I soggetti interessati o non saranno danneggiati dalla violazione o subiranno solo pochi inconvenienti, che potranno superare senza particolari problemi (tempo speso per reinserire le informazioni, fastidi, nervosismo, etc.).
2 ≤ SE < 3	**Media**	I soggetti interessati potrebbero andare incontro a considerevoli inconvenienti, che saranno in grado di superare a fronte di alcune difficoltà (costi ulteriori, impossibilità di accedere a servizi aziendali, timori, problemi nel comprendere cosa sta accadendo, stress, disagi fisici minori, ecc.).
3 ≤ SE< 4	**Alta**	I soggetti interessati potrebbero andare incontro a significative conseguenze, che dovrebbero essere in grado di superare seppur con serie difficoltà e disagi anche gravi (appropriazione indebita di somme di denaro, segnalazione alla centrale rischi del circuito bancario, danni alla proprietà, perdita dell'impiego, indagini da parte della magistratura, peggioramento delle condizioni di salute).
4 ≤ SE	**Molto Alta**	I soggetti interessati potrebbero andare incontro a significative, o addirittura irreversibili, conseguenze, che potrebbero non essere in grado di superare (gravi dissesti economici, come un debito molto elevato, incapacità di lavorare, problemi fisici o psicologici di lungo periodo, morte, etc.).

Brexit: bozza decisione di adeguatezza di Commissione UE

Il 19 febbraio u.s. la Commissione UE ha " … ***launched the process towards the adoption of two adequacy decisions for transfers of personal data to the United Kingdom****, one under the General Data Protection Regulation and the other for the Law Enforcement Directive. The publication of the draft decisions is the beginning of a process towards their adoption. This involves obtaining an opinion from the European Data Protection Board (EDPB) and the green light from a committee composed of representatives of the EU Member States.* ***Once this procedure will have been completed, the Commission could proceed to adopt the two adequacy decisions****.*

Over the past months, the Commission has carefully assessed the UK's law and practice on personal data protection, including the rules on access to data by public authorities. ***It concludes that the UK ensures an essentially equivalent level of protection to the one guaranteed under the General Data Protection Regulation (GDPR) and, for the first time, under the Law Enforcement Directive (LED)*** *… omissis …"*

Il parere di EDPB alla bozza di decisione è stato il seguente:



1.3. Conclusion

The EDPB considers that the UK adequacy assessment is unique because of the previous status of the UK as an EU Member State. Besides, it would also be the first adequacy decision including a sunset clause.

Accordingly, the EDPB recognises many areas of convergence between the UK and the EU data protection frameworks. At the same time, however, and following a careful analysis of the European Commission's draft decision and the UK data protection legislation, the EDPB has identified a number of challenges, which are examined extensively in this opinion. In this context, the EDPB wishes to emphasise the paramount role of the European Commission on the monitoring of all relevant developments in the UK.

In light of the above, the EDPB recommends the European Commission to address the challenges raised in this opinion. The EDPB also invites the European Commission to monitor closely all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data, and to take swiftly appropriate actions, where necessary.

Trasferimenti di dati all'estero: dopo Schrems II

La sentenza «Schreams II» che ha portato all'invalidazione da parte della CGUE dell'accordo sullo scambio di dati personali tra UE e USA ha secondo il prof. Guido Scorza, componente del Garante privacy, una portata ben più vasta « *… Perché – e questo è un dato importante da tenere presente – la situazione che, dopo la Sentenza della Corte di Giustizia, si è venuta a creare tra Bruxelles e Washington non è unica ma è* ***comune a decine di altri Paesi verso i quali i dati personali in partenza dall'Europa possono dover approdare*** *…».*

In questo intervento tralasceremo di considerare le altre possibili basi giuridiche utilizzabili per i trasferimenti di dati all'estero in Paesi non adeguati quali le c.d. «norme vincolanti d'impresa» (art. 47 del GDPR) o le deroghe (vedi le linee guida relative) in specifiche situazioni previste dall'art. 49 del GDPR, per concentrarci sulle novità che si sono registrate nella possibilità di utilizzare quali garanzie adeguate (art. 46 del GDPR) **le clausole tipo di protezione dei dati adottate dalla Commissione UE [SCC(1)]**, sottolineando, che esse sono utilizzabili « ***… a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi****»* che, anche nella nostra esperienza professionale, appaiono le più utilizzate.

(1) Standard Contractual Clauses

Nuove clausole contrattuali standard da Commissione UE

- ✓ Le SCC emanate prima del GDPR sono reperibili sul sito del Garante seguendo il percorso «*home→provvedimenti e normative → Trasferimenti di dati personali*» distinte per trasferimenti da titolare a responsabile (2010) e da titolare a titolare.
- ✓ Ogni modifica o emendamento delle SCC ne comporta la trasformazione in clausole contrattuali ad hoc.
- ✓ Esse rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione UE
- ✓ Una **nuova versione** (ancora non definitiva) **delle SCC è stata approntata dalla Commissione UE** e su di essa sono arrivati i necessari pareri congiunti di EDPS e di EDPB.
- ✓ **Intanto però le Autorità di controllo (DPA) UE si stanno muovendo sul tema** ed in particolare l'Autorità bavarese, a seguito del reclamo di un cittadino che si era visto recapitare una mail per conto di un *magazine* locale, utilizzando il servizio Mailchimp, ha adottato un provvedimento verso la società statunitense, che trovate commentato nell'articolo del giornalista Alessandro Longo intitolato "*Schrems II, prima pronuncia privacy: così Mailchimp in Germania segna un precedente*" (link in bibliografia). Non c'è stata sanzione ma, come conclude l'articolo citato, "*Questa decisione lascia quindi con una certezza: **l'invio dei dati verso gli Stati Uniti, anche se basato su Clausole Contrattuali Standard è illegittimo se non seguito da misure ulteriori."***
- ✓ Relativamente agli specifici rapporti tra UE e USA «"***The U.S. Government and the European Commission have decided to intensify negotiations on an enhanced EU-U.S. Privacy Shield framework to comply with the July 16, 2020 judgment of the Court of Justice of the European Union in the Schrems II case*** … omissis … *".*

Trasferimenti dati all'estero: le raccomandazioni EDPB

EDPB ha pubblicato **due serie di raccomandazioni(1): le prime** contengono una serie di passi che gli esportatori di dati devono seguire per poter trasferire i dati al di fuori dello Spazio Economico Europeo in conformità con il GDPR con un **allegato** che contiene un elenco esemplificativo e non esaustivo di misure tecniche (crittografia, separazione del trattamento, pseudonimizzazione), contrattuali (trasparenza degli obblighi, diritti delle persone) e organizzative (politica interna, trasparenza, procedure), a garanzia del trasferimento; le **seconde** forniscono agli esportatori dei "criteri" per determinare se il **quadro giuridico** che disciplina l'accesso delle autorità pubbliche ai dati personali, a fini di sorveglianza, nei Paesi terzi può essere considerato un'interferenza nel diritto alla protezione dei dati personali

In bibliografia trovate il link ad un articolo di approfondimento sull'uso della «cassetta degli attrezzi» che secondo l'avv. Rocco Panetta è stata messa a disposizione da EDP con le sue Raccomandazioni.

*(1) Le Raccomandazioni di EDPB sopra indicate sono state sottoposte a consultazione pubblica fino al 30 novembre 2020 e sono **applicabili immediatamente dopo la loro pubblicazione**.*

Covid-19 e privacy: Le FAQ del Garante italiano

- ✓ Il "*Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro*» del 24 aprile 2020 consente al datore di lavoro di **rilevare la temperatura corporea all'ingresso dei locali** dell'azienda nonché di **raccogliere dichiarazioni** sugli eventuali contatti avuti negli ultimi 14 giorni con persone affette dal virus
- ✓ La raccolta di tali dati **richiede la resa di una specifica informativa** ai sensi dell'art. 13 GDPR
- ✓ Il Garante privacy ha pubblicato delle FAQ su «Covid-19 e protezione dei dati» in una delle quali è precisato:

> **6. Può essere resa nota l'identità del dipendente affetto da Covid-19 agli altri lavoratori da parte del datore di lavoro?**
>
> No. In relazione al fine di tutelare la salute degli altri lavoratori, in base a quanto stabilito dalle misure emergenziali, spetta alle autorità sanitarie competenti informare i "contatti stretti" del contagiato, al fine di attivare le previste misure di profilassi.
>
> Il datore di lavoro è, invece, tenuto a fornire alle istituzioni competenti e alle autorità sanitarie le informazioni necessarie, affinché le stesse possano assolvere ai compiti e alle funzioni previste anche dalla normativa d'urgenza adottata in relazione alla predetta situazione emergenziale (cfr. paragrafo 12 del predetto Protocollo).

- ✓ Anche le attività di vaccinazione in azienda consentite dal «*Protocollo nazionale per la realizzazione dei piani aziendali finalizzati all'attivazione di punti straordinari di vaccinazione anti SARS-CoV-2/Covid-19 nei luoghi di lavoro*» del 6 aprile 2021 dovranno essere svolte nel pieno rispetto delle norme in materia di tutela della riservatezza e della sicurezza mentre il medico competente assicura la registrazione delle vaccinazioni eseguite mediante gli strumenti messi a disposizione dai Servizi Sanitari Regionali, nel rispetto delle vigenti disposizioni per la tutela della riservatezza dei dati personali,

Conferenze on-line: consigli da Garante privacy spagnolo (1)

L'Autorità di controllo spagnola (AEPD) ha pubblicato i suoi consigli per la privacy e la sicurezza delle riunioni on line:

- ✓ Osserva e segui le politiche stabilite dalla tua organizzazione per le riunioni online. Questo include l'utilizzo solo del fornitore di tecnologia approvato dall'organizzazione.
- ✓ Nelle riunioni con un gran numero di partecipanti e da più organizzazioni, è una buona idea designare almeno un partecipante per assistere l'organizzatore durante la riunione nel controllo dei partecipanti e nelle questioni di privacy e sicurezza.
- ✓ Pensate in anticipo alla sensibilità degli argomenti da discutere, all'identità dei partecipanti e al potenziale di diffusione se la riunione viene registrata.
- ✓ Limitare il riutilizzo dei codici di accesso/link. Se lo stesso codice/link è stato usato per un po', probabilmente lo avete condiviso con più persone di quante possiate immaginare o ricordare.
- ✓ Se l'argomento della riunione è sensibile, sia per l'argomento, sia per l'identità dei partecipanti, o per qualsiasi altra questione, usate codici, collegamenti url e/o pin di accesso monouso. Inoltre, considerate la necessità di utilizzare l'autenticazione a due fattori. Questo impedirà a qualcuno di potersi iscrivere semplicemente scoprendo l'URL del collegamento o il codice di accesso.
- ✓ Disabilita le funzionalità non necessarie come la chat, la condivisione dei file o dello schermo.
- ✓ Se applicabile, limitate chi può condividere il vostro schermo per evitare immagini indesiderate o inaspettate. Prima che qualcuno condivida il suo schermo, ricordategli il rischio di condividere informazioni sensibili.
- ✓ Indirizza la chiamata solo a contatti specifici, evitando di inviare chiamate a gruppi o mailing list, che includono collegamenti che sono validi solo perché sono in loro possesso.
- ✓ Usate una "sala d'attesa" per ammettere i partecipanti, e non permettete che la riunione cominci finché l'ospitante non si unisce alla riunione.

Conferenze on-line: consigli da Garante privacy spagnolo (2)

- ✓ Abilita la notifica per quando i partecipanti si uniscono alla riunione. Questo potrebbe essere un tono distintivo o l'annuncio del loro nome. Se il tuo provider non lo permette, assicurati che l'ospitante chieda ai nuovi partecipanti di identificarsi.
- ✓ Se disponibile, usa un pannello per controllare i partecipanti e identificare quelli che sono generici.
- ✓ Non registrare la riunione a meno che non sia necessario. In tal caso, informate adeguatamente i partecipanti dello scopo della registrazione e del punto in cui la registrazione inizia/si ferma. Alcuni venditori fanno questi annunci automaticamente.
- ✓ Prima di iniziare la riunione, controllate quale area è visibile dietro di voi e quali informazioni personali state rivelando. Considerate l'uso di uno sfondo virtuale per mascherare lo sfondo.
- ✓ Avvisate i potenziali collaboratori che sta per iniziare una riunione e prendete provvedimenti per tenere la vostra attività fuori dalla portata del microfono e della telecamera.
- ✓ Al di là delle questioni di efficienza della comunicazione, durante la riunione spegnete il microfono e la ripresa video quando non è necessario. In particolare, se avete intenzione di eseguire qualsiasi azione al di fuori della messa a fuoco della telecamera. Presti particolare attenzione ai microfoni senza fili.
- ✓ Siate consapevoli che la cattura video e audio può continuare, a causa di qualche tipo di errore umano o di sistema, quando pensate che la riunione sia finita.
- ✓ Quando la riunione è finita, assicurati di usare un dispositivo che disabiliti fisicamente la telecamera (scheda, adesivo o simile). Non rimuovete il dispositivo finché non state per iniziare la connessione.

Agenda

- Presentazione relatore
- GDPR due anni dopo
- **Bibliografia & sitografia**
- Q&A

Bibliografia & Sitografia

Data breach
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en

https://www.cybersecurity360.it/legal/privacy-dati-personali/credential-stuffing-e-mancato-contrasto-al-furto-dati-online-la-cnil-sanziona-i-gestori-di-un-sito-web/

Brexit
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661
https://edpb.europa.eu/our-work-tools/our-documents/other/opinion-142021-regarding-european-commission-draft-implementing_en

Trasferimenti dati personali all'estero
https://www.agendadigitale.eu/sicurezza/privacy/trasferimento-dati-extra-ue-abbiamo-un-problema-anzi-tre-e-non-riguarda-solo-gli-usa/
https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_en
https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edpb-edps_pressrelease_onsccs_en.pdf
https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443
https://www.cybersecurity360.it/legal/privacy-dati-personali/schrems-ii-prima-pronuncia-europea-cosi-mailchimp-in-germania-segna-un-precedente/
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en
https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en
https://www.corrierecomunicazioni.it/privacy/schrems-ii-in-arrivo-la-cassetta-degli-attrezzi-panetta-ruolo-dei-dpo-sempre-piu-importante/

COVID-19 e privacy
https://www.garanteprivacy.it/temi/coronavirus/faq
http://www.salute.gov.it/imgs/C_17_pagineAree_5383_1_file.PDF

Privacy nelle riunioni online
https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-reuniones-online

Agenda

- Presentazione relatore
- Protezione dei dati personali: panoramica su recenti evoluzioni normative
- Bibliografia & sitografia
- Q&A

Agenda

- Presentazione relatore
- Protezione dei dati personali: panoramica su recenti evoluzioni normative
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it

Grazie...