PERSONAL DATA BREACH? DO NOT FORGET TO NOTIFY!

PROF. SYLVAIN MÉTILLE

ASSOCIATION OF INTERNATIONAL BUSINESS LAWYERS

GENEVA, NOVEMBER 26, 2021

lematin.ch

Vidéo Radio Cockpit

Home Suisse Sports Faits divers Monde People Loisirs Plus

CYBERATTAQUE

23.09.2020 à 16:41

Des pirates dérobent les données de 11'000 passeports suisses

Des cyberescrocs ont volé les données des passeports de quelque 11'000 ressortissants suisses ayant voyagé en Argentine et les ont publiées sur le darknet. L'Office fédéral de la police estime que cette cyberattaque ne représente qu'un faible risque d'abus.

Des pirates informatiques sont parvenus à dérober des données du service d'immigration argentin concernant plus de 11'000 passeports suisses.
KEYSTONE

ICTjournal

NEWS

Faille de sécurité

Des clients de Digitec.ch victimes d'un vol de données personnelles

Lun 20.11.2017 - 11:21
par Yannick Chavanne

Des clients de l'e-boutique suisse Digitec, filiale de Migros, ont été victimes d'un vol de données personnelles.

AddThis

Siège de Digitec Galaxus AG à Zurich. (Source: Digitec Galaxus)

Des escrocs sont en possession des données personnelles de clients de la boutique en ligne suisse Digitec. Une information rapportée par le site Watson.ch et à laquelle la filiale de Migros n'a pas tardé à réagir officiellement, confirmant une fuite de données.

LE TEMPS

29 sep. 2020

SERVICES S'ABONNER

TECHNOLOGIE

Pourquoi le vol de données de 800000 clients de Swisscom n'est pas anodin

Les données de 800 000 clients, dont leurs nom, date de naissance et numéro de téléphone mobile, ont été volées chez un partenaire de l'opérateur. Ces informations pourraient être utilisées pour commettre des actes délictueux

Les données volées, mêmes jugées non sensibles, peuvent permettre de faire du «social engineering» et de se faire par exemple passer pour un client de Swisscom pour obtenir ensuite des données de carte de crédit. — © 123rf

LE TEMPS

SE CONNECTER SERVICES S'ABONNER

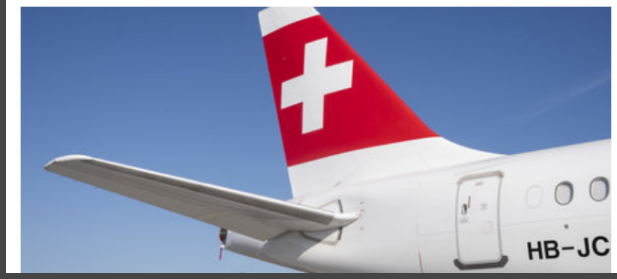
RUBRIQUES EN CONTINU BLOGS VIDÉOS CHAPPATTE MULTIMÉDIA EPAPER/PDF

Accueil › Economie › Le piratage de Swiss, symbole de la hausse du nombre de cyberattaques

TECHNOLOGIE ABONNÉ

Le piratage de Swiss, symbole de la hausse du nombre de cyberattaques

Les données de 1,35 million de passagers, dont des clients de la compagnie aérienne helvétique, ont été volées. Les Swiss Cyber Security Days, qui se tiennent jusqu'à ce jeudi soir, sont l'occasion de mettre en lumière ces menaces grandissantes



FRAMEWORK

- The Federal Act on Data Protection (FADP) applies to the processing of personal data. It aims to protect the personnality of the data subjects.
- Data must always be processed in accordance with the following principles : lawfulness, fairness/good faith, proportionality, purpose, transparency and security.
- The revised FADP (nFADP) has been adopted on September 25, 2020 (entry into force expected in January 2023).

ART. 8 NFADP (SECURITY)

Art. 8 Data security

[1] The controller and the processor must ensure, through adequate technical and organisational measures, security of the personal data that appropriately addresses the risk.

[2] The measures must enable the avoidance of data security breaches.

[3] The Federal Council shall issue provisions on the minimum requirements for data security.

SECURITY PRINCIPLE

- Integrity
- Confidentiality
- Availability

PERSONAL DATA BREACH

- Any breach of security…
- …resulting in the accidental or unlawful loss, alteration, deletion, destruction, disclosure or unauthorised access of personal data (art. 5 lit. h nFADP)

PERSONAL DATA BREACH NOTIFICATION

Art. 24 Notification of data security breaches

[1] The controller shall notify the FDPIC as soon as possible of a data security breach that is probable to result in a high risk to the personality rights or the fundamental rights of the data subject.

[2] In the notification, it must at least indicate the nature of the data security breach, its consequences and the measures taken or foreseen.

[3] The processor shall notify the controller as soon as possible of any data security breach.

[4] The controller shall also inform the data subject if this is necessary for the protection of the data subject or if the FDPIC so requests.

[5] It can restrict the information to the data subject, defer it or refrain from providing information if:

a. there are grounds pursuant to Article 26 paragraph 1, letter b or 2 letter b or a statutory duty of secrecy prohibits it;
b. information is impossible or requires disproportionate efforts; or
c. the information of the data subject is ensured in an equivalent manner by a public announcement.

[6] A notification based on this Article can be used in criminal proceedings against the person subject to notification only with such person's consent.

NOTIFICATION

- By the controller
  - to the Federal Data Protection and Information Commissioner (FDPIC)
    - in case of a high risk for the privacy or the fundamental rights of the data subjects
  - to the data subjects
    - if necessary for their protection
- By the processor
  - to the controller in any case

NOTIFICATION CONTENT

- Nature of the breach
- Consequences of the breach
- Steps taken or proposed

EXCEPTIONS

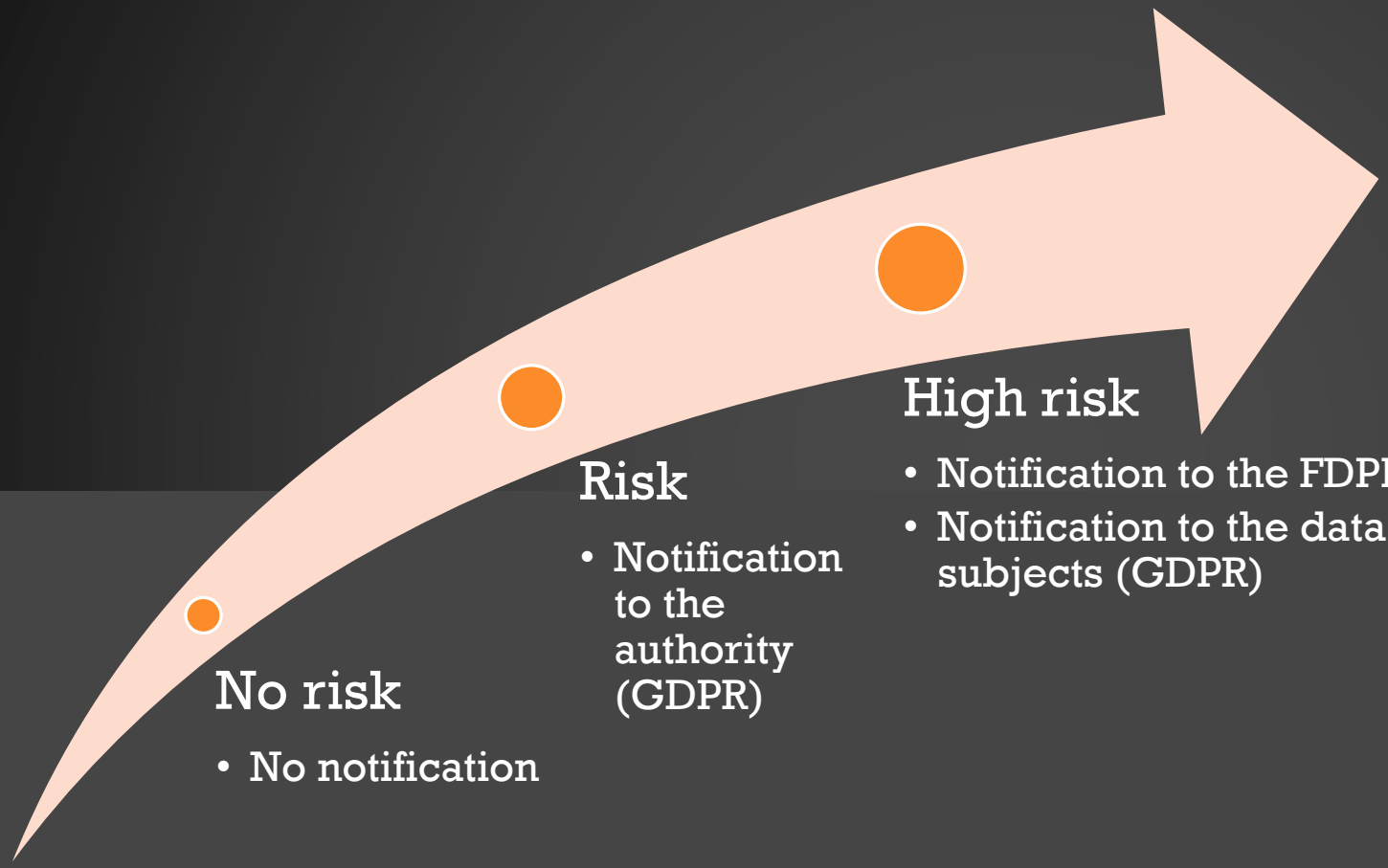
- No obligation to notify in the absence of high risk (for the privacy or fundamental rights of the data subjects)
- Possibility to restrict, defer, or abstain from informing the data subject (not the FDPIC) if:
  - the interests of third parties require it;
  - the information is impossible to give or requires disproportionate efforts;
  - the information of the data subject can be equally safeguarded by a public announcement;
  - this is required to protect overriding public interests or the information would jeopardise the outcome of a criminal investigation or any other investigation proceedings (federal bodys only).

SANCTIONS

- No criminal / administrative sanction for failing to notify
- A notification can only be used in a criminal proceeding against the person subject to notification with his/her their consent (art. 24 al. 6 nFADP).
- The FDPIC can order the data controller to notify him and, if needed, to inform the data subjects pursuant to art. 24 (art. 51 al. 3 let. f nFADP), if necessary under the threat of art. 63 nFADP (non-compliance with a decision).

NFADP VS GDPR

	Art. 24 nFADP	**Art. 33 and 34 GDPR**
Time of notification	Without undue delay	Without undue delay *and, where feasible, not later than 72 hours after having become aware of it*
Notification to the FDPIC /supervisory authority	Breach *likely to result in a high risk* to the privacy or the fundamental rights of the data subject	Any breach *except* if *unlikely to present a risk* to the rights and freedoms of natural persons
Notification to the data subject	Whenever necessary for their protection	Whenever a breach is likely to present a risk to their rights and freedoms
Sanction	No administrative sanction	Administrative fines up to *EUR 10 000 000.- or 2%* of the total worldwide annual turnover of the preceding financial year (art. 83 GDPR)



No risk

- No notification

Risk

- Notification to the authority (GDPR)

High risk

- Notification to the FDPIC
- Notification to the data subjects (GDPR)

+ Notification to the data subjects irrespective of the risk if necessary for their protection

A FEW FINES

- The CNIL conducts inspections based on identified IP addresses.
- Fines of EUR 6 000.- and 3 000.- imposed on doctors for opening the ports of their LiveBox in order to run a VPN and thus creating an access to their computers which contained medical images.
- The fine covers the violation of the obligation to ensure data security and the violation of the obligation to notify a data breach (eventhough the CNIL actually informed them of the breach during an inspection).

PRESS RELEASES

45M Medical Images Accessible Online

CybelAngel • December 14, 2020

More Than 45 Million Medical Images Openly Accessible Online

CybelAngel identifies medical devices and web portals leaking unprotected images including X-rays and CT Scans

PARIS and NEW YORK, December 15, 2020 – The analyst team at CybelAngel, a global leader in digital risk protection, has discovered that more than 45 million medical imaging files – including X-rays and CT scans – are freely accessible on unprotected servers, in a new research report released today. The report "Full Body Exposure" is the result of a six-month investigation into Network Attached Storage (NAS) and Digital Imaging and Communications in Medicine (DICOM), the de facto standard used by healthcare professionals to send and receive medical data. The analysts discovered millions of sensitive images, including personal healthcare information (PHI), were available unencrypted and without password protection.

CybelAngel tools scanned approximately 4.3 billion IP addresses and detected more than 45 million unique medical images left exposed on over 2,140 unprotected servers across 67 countries including the US, UK, France and Germany.

The analysts found that openly available medical images, including up to 200 lines of metadata per record which included PII (personally identifiable information; name, birth date, address, etc.) and PHI (height, weight, diagnosis, etc.), could be accessed without the need for a username or password. In some instances login portals accepted blank usernames and passwords.

News > Dutch DPA fines Booking.com for delay in reporting data breach

Dutch DPA fines Booking.com for delay in reporting data breach

9 April 2021

Netherlands

The Dutch Data Protection Authority (DPA) has imposed a €475,000 fine on Booking.com because the company took too long to report a data breach to the DPA. When the breach occurred, criminals obtained the personal data of over 4,000 customers. They also got their hands on the credit card information of almost 300 people.

In a telephone scam targeting 40 hotels in the United Arab Emirates in December 2018, the criminals persuaded hotel staff to reveal the log-in details for their accounts in a Booking.com system. In this way the criminals gained access to the data of 4,109 people who had booked a hotel room in the UAE. The data included their names, addresses and telephone numbers, as well as details of their booking.

The criminals were also able to access the credit card information of 283 people. In 97 cases, the credit card security code was obtained as well. The criminals also tried to get hold of the credit card information of other victims, by posing as Booking.com staff in emails or on the telephone.

Phishing

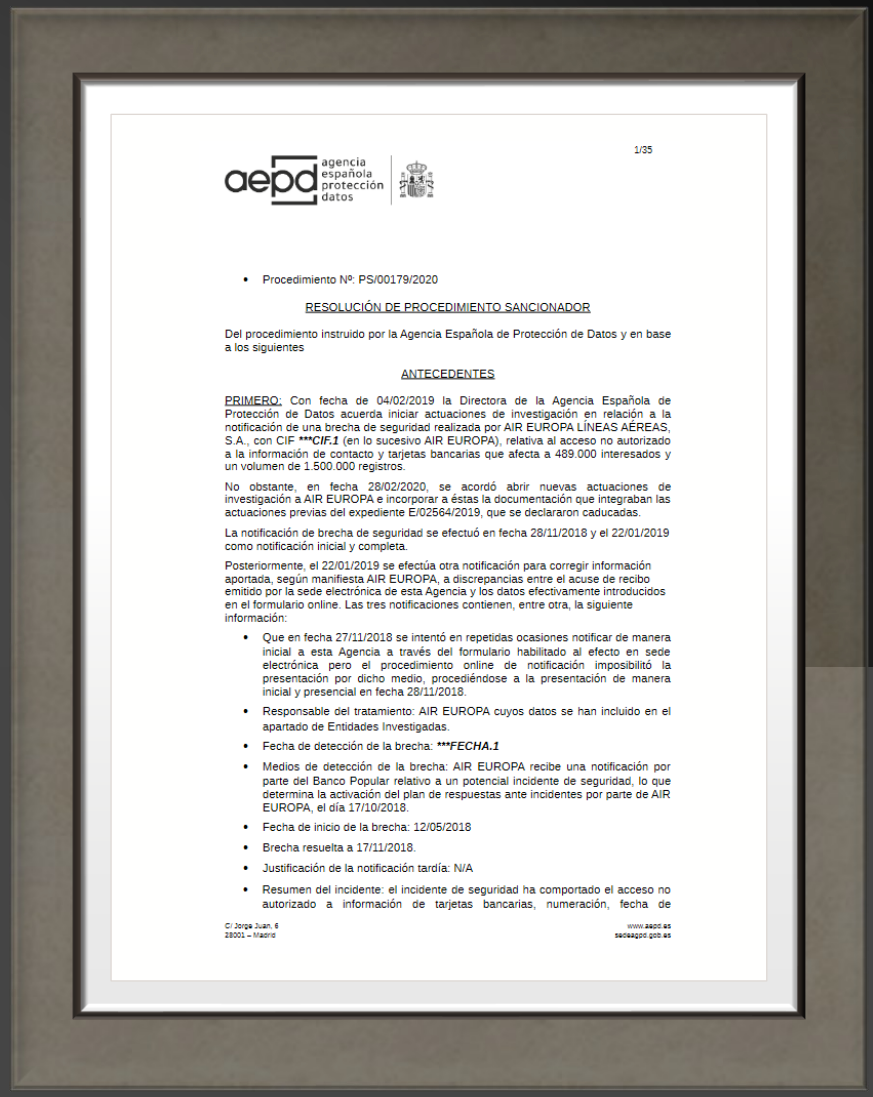
'Booking.com customers ran a risk of falling victim to serious theft,' says DPA deputy chair Monique Verdier, 'even if the criminals didn't obtain edit card information but only someone's name, contact details and

A FEW FINES

- EUR 475 000.- fine imposed on by the Dutch authority (Autoriteit Persoonsgegevens) on Booking.com for delay in reporting data breach (22 days after having become aware of it), a breach affecting 4 000 clients (names, addresses, phone numbers and approx. 300 credit card numbers)

A FEW FINES

- Fine imposed on 17.03.2021 by the Spanish authority (AEPD) on Air Europa Lineas Aereas, SA because of an unauthorised access to contact details and bank accounts (489 000 individuals et 1 500 000 data records)
  - EUR 500 000.- for their failure to have in place appropriate technical and organisational measures
  - EUR 100 000.- for notifying the breach with a delay of 41 days



1/35

aepd agencia española protección datos

- Procedimiento Nº: PS/00179/2020

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 04/02/2019 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación en relación a la notificación de una brecha de seguridad realizada por AIR EUROPA LÍNEAS AÉREAS, S.A., con CIF ***CIF.1 (en lo sucesivo AIR EUROPA), relativa al acceso no autorizado a la información de contacto y tarjetas bancarias que afecta a 489.000 interesados y un volumen de 1.500.000 registros.

No obstante, en fecha 28/02/2020, se acordó abrir nuevas actuaciones de investigación a AIR EUROPA e incorporar a éstas la documentación que integraban las actuaciones previas del expediente E/02564/2019, que se declararon caducadas.

La notificación de brecha de seguridad se efectuó en fecha 28/11/2018 y el 22/01/2019 como notificación inicial y completa.

Posteriormente, el 22/01/2019 se efectúa otra notificación para corregir información aportada, según manifiesta AIR EUROPA, a discrepancias entre el acuse de recibo emitido por la sede electrónica de esta Agencia y los datos efectivamente introducidos en el formulario online. Las tres notificaciones contienen, entre otra, la siguiente información:

- Que en fecha 27/11/2018 se intentó en repetidas ocasiones notificar de manera inicial a esta Agencia a través del formulario habilitado al efecto en sede electrónica pero el procedimiento online de notificación imposibilitó la presentación por dicho medio, procediéndose a la presentación de manera inicial y presencial en fecha 28/11/2018.
- Responsable del tratamiento: AIR EUROPA cuyos datos se han incluido en el apartado de Entidades Investigadas.
- Fecha de detección de la brecha: ***FECHA.1
- Medios de detección de la brecha: AIR EUROPA recibe una notificación por parte del Banco Popular relativo a un potencial incidente de seguridad, lo que determina la activación del plan de respuestas ante incidentes por parte de AIR EUROPA, el día 17/10/2018.
- Fecha de inicio de la brecha: 12/05/2018
- Brecha resuelta a 17/11/2018.
- Justificación de la notificación tardía: N/A
- Resumen del incidente: el incidente de seguridad ha comportado el acceso no autorizado a información de tarjetas bancarias, numeración, fecha de

C/ Jorge Juan, 6
28001 – Madrid

www.aepd.es
sedeagpd.gob.es

MANAGING A SECURITY BREACH CANNOT BE IMPROVISED

- You need a plan
  - Incident management process
  - Technical detection and feedback
  - Analyse, qualify and act
  - Communication
  - Learn from experience

CONCLUSION

- A personal data breach will occur.
  - Are you ready?
- Management is complex and time is short.
  - It is better to know your obligations and have a procedure in place.
- There is no need to wait for the entry into force of the revised FADP to be prepared.

SYLVAIN MÉTILLE

- HDC
  - Avocat associé
- Université de Lausanne
  - Professeur associé
  - Directeur de la Maîtrise universitaire en Droit, criminalité et sécurité des technologies de l'information (M DCS)
  - Membre de la Commission d'éthique de la recherche de l'Université de Lausanne (CER-UNIL)
- UniDistance
  - Responsable scientifique et Chargé d'enseignement (CAS protection des données)
- Contact: @smetille, metille@hdclegal.ch, www.smetille.ch

HDC
LAW FIRM
ÉTUDE D'AVOCATS

Unil
UNIL | Université de Lausanne

FORMATION UNIVERSITAIRE
A DISTANCE, SUISSE