itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Schulungsworkshop DS-GVO

Pragmatischer Ansatz

30/03/2018

C. Harpes
M. Aubigny

itrust consulting s.à r.l.
55, rue Gabriel Lippmann
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Einleitung

DS-GVO Schulung

Agenda

Organisation der Schulung (9:15-9:20)

Allgemeiner Ansatz (9:20-10:20)

- Ziel der DS-GVO Gewährleistung der Rechte der berechtigten Personen (bPerson)
- Erreichen des Ziels: Die 7 allgemeinen Grundsätze zur Behandlung von pbD

Kaffeepause (10:20-10:40)

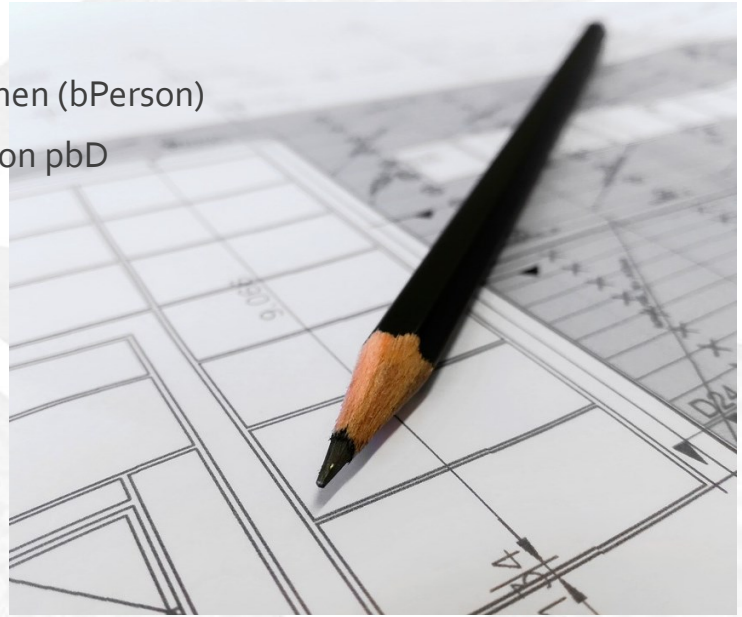
Allgemein Suite-Ansatz (10:45-11:45)

- Erinnerung: Was sind personenbezogene Daten (pbD)?
- Einwilligung: wann und wie?

Imbiss (11:45-12:15)

Und in der Praxis….

- Gute Reflexe
- Präsentation der Workshops: Dokumente & Vorbereitung?



Es gibt keine schlechten Fragen: zögern Sie nicht, während der Vorträge einzugreifen.

itrust consulting

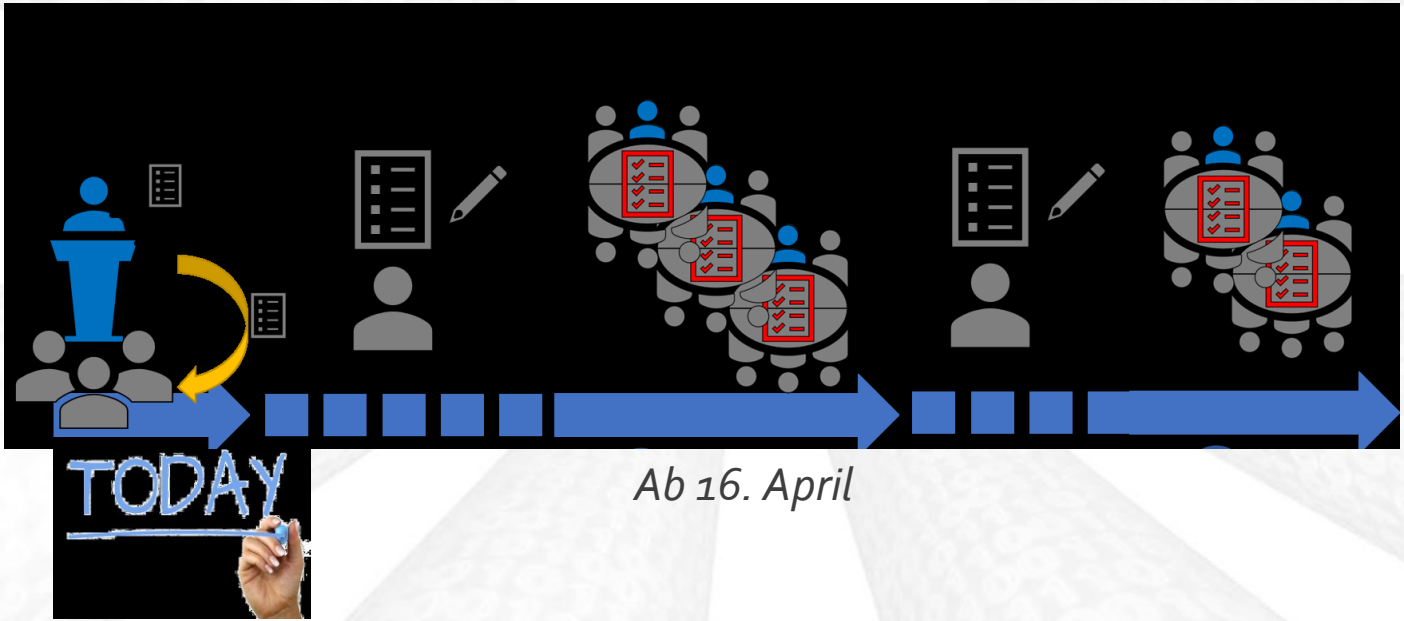
FEDERATION DES ARTISANS

Move securely within the cyberworld

Organisation der DS-GVO Schulung

Organisation der DS-GVO Schulung

Praktische Organisation der Workshops



Ab 16. April

Die Workshops

Register der Verarbeitungsvorgänge	16/04 : 9h-11h 24/04 : 13h-15h	Verwaltung und Benachrichtigung bei Sicherheitsverletzungen
Datenschutzerklärung	16/04 : 11h-13h 24/04 : 15h-17h	Verwaltung von pbD-Auftragsverarbeitern und Vertragsklauseln
Verhaltenskodex für Daten und IT-Benutzer	23/04 : 9h-11h 25/04 : 9h-11h	Datenklassifikation und Prozeduren
Einwilligung	23/04 : 11h-13h 25/04 : 11h-13h	Dokumentenverwaltung

Anmeldung bei der FdA.

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Allgemeiner Ansatz der DS-GVO

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Ziel der DS-GVO

Gewährleistung der Rechte der bPersonen

Ziel der DS-GVO « *Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (pbD).*

Zu diesem Zweck sind die Regeln, die für alle Verarbeitungen gelten, so konzipiert, dass dies gewährleistet ist:

Recht auf Transparenz	Recht auf Einschränkung der Verarbeitung	Widerspruchsrecht gegen die Verarbeitung
Recht auf Informationen	Recht auf Löschung („Vergessenwerden“)	
Recht auf Berichtigung	Recht auf Datenübertragbarkeit	

Gewährleistung der Rechte: Berichtigung & Löschung

Recht auf Berichtigung: schnellstmögliche Berichtigung oder Fertigstellung

Recht auf Löschung („auf Vergessenwerden") Löschung so bald wie möglich, wenn eine der Bedingungen erfüllt ist:

1. Daten werden für die Zwecke der Verarbeitung nicht benötigt.
2. Die Einwilligung wurde widerrufen.
3. Die bPerson widerspricht der Verarbeitung.
4. Die Verarbeitung war rechtswidrig.
5. Gesetzliche Verpflichtung
6. Erhebung betraf "Minderjährigen" (<16 Jahre), der mit 16 Jahren die Daten löschen will.

Falls die Daten veröffentlicht wurden: Löschung der Daten und aller Kopien (unter Berücksichtigung von Technologie und Kosten)

Verweigerung der Löschung: wegen Meinungsfreiheit, rechtlicher Verpflichtung, öffentlichem Interesse, Archivierung oder Verteidigung.

Gewährleistung der Rechte: Datenübertragbarkeit

Recht auf Datenübertragbarkeit: Recht auf Wiederherstellung von Daten in **einem strukturierten,** wiederverwendbaren Format, Recht auf Übermittlung an einen anderen für die Verarbeitung Verantwortlichen falls:

- auf der Grundlage einer Einwilligung oder eines Vertrages.
- auf automatisierten Mitteln (dies gilt nicht für die Papierverarbeitung).

Hinweis: Vom Verantwortlichen zur bPerson (direkter Download) oder an einen anderen Verantwortlichen.

Welche Daten, welche Erhebung? (Art 20.1)

1. pbD der bPerson *(einschließlich pseudonymisierter Daten)*
2. Daten, die von der bPerson während der Verarbeitung erzeugt werden *(Daten, die während der Verarbeitung oder Nutzung des Dienstes erzeugt oder gesammelt werden, einschließlich INDIVIDUELLER Verhaltensanalysedaten*).
3. **Einschränkung**: Wenn die Daten pbD anderer Personen enthalten und deren Rechte verletzt würden.

Übermittlung ≠ Löschen:

(WG Art29 16/EN/WP242)

Gewährleistung der Rechte: Datenübertragbarkeit

Regeln:

1. Verpflichtung des Verantwortlichen, die bPerson über dieses Recht zu informieren (Art.13.2b & 14.2.c).
   Bewährte Praxis: Informieren Sie die bPerson vor der endgültigen Schließung ihres Kontos.
2. Identifizierung der bPerson vor der Beantwortung des Antrags:
   Auskunftspflicht aber keine formale Regelung in der DS-GVO.
   Im Zweifelsfall: zusätzliche Informationen anfordern, um den Antragsteller als bPerson zu identifizieren.
3. Antwortzeit auf die Anfrage: angemessene Frist (<1 Monat nach Eingang), ob positiv oder negativ

Ablehnungen/Zahlung/Zeitrahmen:

1. Ablehnung oder Zahlung: nur bei ungerechtfertigten und wiederholten Anfragen möglich.
2. Fristen: Falls die Datenmenge die normale Übertragungskapazität überschreiten würde, kann eine Frist gewährt werden, um eine geeignetere Methode (CD/DVD-Brennen usw.) zu verwenden. Maximale Frist: 3 Monate

(WG Art29 16/EN/WP242)

Gewährleistung der Rechte: Datenübertragbarkeit

Datenübermittlung – Wie?

1. Format: muss eine Wiederverwendung zulassen. (Art 20.1); maschinenlesbares strukturiertes Format.
   Entscheidend ist die **Interoperabilität** der Lösungen, nicht die genaue Buchhaltung.
2. Metadaten: so viele Metadaten wie nötig und mit ausreichender Granularität für Wiederverwendung bereitstellen *(E-Mails im PDF-Format ist nicht ausreichend).*
3. Bei großen oder komplexen Erhebungen: keine Antwort in der DS-GVO, jedoch müssen die Informationen des für die Verarbeitung Verantwortlichen ausreichen, damit die bPerson seine Daten wiederverwenden kann.
4. Datensicherung während und nach ihrer Übertragung:
   a) Stellen Sie sicher, dass die Daten die Person tatsächlich erreichen, ohne dass die Gefahr des Abfangens besteht.
   b) Informieren Sie die bPerson über die Notwendigkeit, ihre Informationen zu schützen.
   Bewährte Praxis:Daten in einem verschlüsselten Container bereitzustellen.

Hinweis: Eine Lösung zur Erfüllung der Datenübertragbarkeitsanforderungen kann die Implementierung eines sicheren und dokumentierten API sein.

(WG Art29 16/EN/WP242)

Gewährleistung der Rechte: Datenübertragbarkeit

Widerspruchsrecht: Recht, der Verarbeitung (Artikel 6.1.e+f) jederzeit zu widersprechen:

- falls besonderen Situation der bPerson, oder
- bei Direktwerbung (einschliesslich Profiling).

Der Verantwortliche kann sich weigern

- wenn berechtigte und zwingende Gründe die Rechte und Interessen der bPerson außer Kraft setzen
- bei der Ausübung oder Verteidigung vor Gericht
- wenn (im Falle der Verarbeitung für wissenschaftliche oder historische Forschung oder statistische Verarbeitung) die Verarbeitung auf einer öffentlichen Aufgabe beruht.

Pflicht des Verantwortlichen: Information über das Widerspruchsrecht

NB: kann über automatisierte Vorgehensweise erfolgen, sofern konform zur ePrivacy-Richtlinie.

(WG Art29 16/EN/WP242)

itrust consulting

FEDERATION DES ARTISANS

Move securely within the cyberworld

Das Ziel erreichen: Die 7 Grundsätze der DS-GVO

Allgemeine Grundsätze für die Verarbeitung von pbD

7 Grundsätze der Verarbeitungsdurchführung (vgl. Art. 5)

Rechtmäßigkeit/Treu und Glauben/Transparenz

Verantwortung
Rechenschaftspflicht

Beschränkung des Verarbeitungszwecks

Integrität und Vertraulichkeit

Datenminimierung

Speicherung (Einschränkung)

Richtigkeit

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

Die Verarbeitung ist i.a. rechtmäßig, bei einer der folgenden Rechtsgrundlagen:

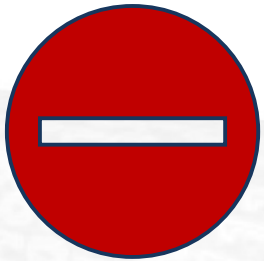
1. Einwilligung
2. Vertrag
3. gesetzlicher Verpflichtung(en)
4. lebenswichtigem Interesse
5. Auftrag von öffentlichem Interesse
6. Ausgehend von berechtigten Gründen (Interessenausgleich)

N. B. Gewöhnlich basiert eine Verarbeitung auf **einer einzigen Rechtsgrundlage,** je nach Art können mehrere gelten.

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

Die Verarbeitung sensibler Daten ist **VERBOTEN**, außer: (Art. 9)

1. aufgrund **ausdrücklicher Zustimmung**
2. im Rahmen des **Arbeits-, Sozialversicherungs- oder Sozialschutzrechts**
3. zur Wahrung der **lebenswichtigen Interessen** der Person
4. für eine **gemeinnützige** Organisation
5. **offensichtlich bekannt** gemacht
6. im Rahmen der **Abwehr eines Rechtsanspruchs**
7. aus **medizinischen oder verwandten Gründen**
8. aus Gründen der **öffentlichen Gesundheit**
9. für **Archivierung, Recherche oder Statistik**
10. im Rahmen der **"nationalen" Gesetzgebung**, insbesondere im Bereich der genetischen Daten, Biometrie etc.



Ad 10: Verarbeitung kann sowohl zulassen als auch eingeschränkt werden.

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

Verarbeitung von Daten über **Verurteilungen und Straftaten:**

nur unter der Kontrolle (oder Ausdrücklicher Genehmigung) der Behörde (Art. 10).

Sonderfälle (cf. DS-GVO)

1. journalistische Zwecke oder akademische, künstlerische oder literarische Ausdrucksformen (Art. 85)
2. Daten in amtlichen Dokumenten (Art. 86)
3. nationale Identifikationsdaten (Art. 87)
4. Archivzwecke von öffentl. Interesse, für wissenschaftliche, historische o. statistische Untersuchungen (Art. 88)
5. Basierend auf der ePrivacy-Richtlinie (in Arbeit bis 25. Mai):
    a) Cookies,
    b) Verkehrsdaten
    c) Standortdaten
    d) Direktmarketing
6. Für Daten über Kinder (<16 Jahre)

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

Die Verarbeitung und die Informationen über die Verarbeitung müssen sicherstellen:

1. Leichte Zugänglichkeit
2. Einfaches Verständnis
3. Klare und einfache Terminologie
4. Identität der Verantwortlichen
5. Über den/die Zweck(e) der Verarbeitung
6. Recht auf Bestätigung und Übermittlung der verarbeiteten pbD
7. Zu Risiken, Regeln, Garantien und Rechten im Zusammenhang mit der Verarbeitung
8. Zu den Bedingungen für die Ausübung ihrer Rechte
9. Werden Transaktionen aufgezeichnet, um Missbrauch zu verhindern?

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

Artikel 12:

Informationen und Übermittlungen im Zusammenhang mit der Verarbeitung pbD müssen:

1. übersichtlich, transparent, verständlich und leicht zugänglich (12.1)
2. in klarer und einfacher Sprache (12.1)
3. mit besondere Aufmerksamkeit für Kinder (12.1)
4. geschrieben (12.1)
5. mündlich (12.1)
6. kostenlos (12.5) sein

Säule 1: Rechtmäßigkeit, Treu und Glauben, Transparenz

1. Übersichtlich, transparent: klar getrennt von anderen Verarbeitungsbedingungen (Erklärung, Charta, Politik)....
2. Verständlich: muss für einen durchschnittlichen Leser verständl (Zuhörer)
3. Leicht zugänglich: Die bPerson sollte nicht suchen müssen.
4. Klartext bedeutet Information in einer Sprache, die komplexe S (lange Sätze mit Nebensätzen) vermeidet, ohne Abstraktion od Ambivalenz von Begriffen (keine Interpretation möglich).

Ein paar Regeln:

a) Vermeiden Sie "kann sein", "könnte sein", "einige", "möglich".
b) Aktiver und nicht passiver Satzbau verwenden
c) Kein juristisches, technisches oder fachspezifisches Vokabular
d) Konsistenz bei mehreren Sprachen prüfen (Transliteration vermeiden)

Säule 2: Zweckbegrenzung

Primäre Zwecke (bei Erhebung festgelegt), sind

1. spezifische
2. explizite
3. berechtigt
4. dokumentiert

Sekundäre Zwecke (nach der Erhebung vor Verarbeitung der pbD):

Kompatible Zwecke :

1. Archivierung von öffentlichem Interesse oder für wissenschaftliche, historische oder statistische Recherchen.
2. Basierend auf der initialen Einwilligung
3. Aufgrund gesetzlicher Verpflichtung

Wenn nicht: Zweckkompatibilität erstellen basierend auf:

1. Verknüpfung mit einem primärem Zweck
2. Spezifischer Beziehung zwischen bPerson und dem Verantwortlichen
3. die Art der Daten
4. ein kausaler Zusammenhang zwischen Verarbeitungen
5. Sicherheitsmaßnahmen wie Verschlüsselung und Pseudonymisierung

Säule 2: Zweckbegrenzung

Das Prinzip der Einschränkung der Verarbeitung pbD verpflichtet sowohl den Verantwortlichen und den pbD-Auftragsverarbeiter als auch den IT-Dienstleister. Maßnahmen zu ergreifen, um die Nutzung von pbD für einen anderen Zw einzuschränken.

Für Verantwortlichen und pbD-Auftragsverarbeiter:

1. Spezifische oder minimale Maßnahmen zur Vermeidung oder Erschwerung Verwendung von Daten für einen anderen Zweck
2. Verhindert oder erschwert die Verwaltung des Zugriffs die Verwendung für and Zwecke?

Für den IT-Lösungsanbieter (Service, Software oder System)

1. Konzeption der Lösung zur Vermeidung einer zweckfremden Verwendung
2. Informationen und Verhaltenskodex zur Förderung der Anwendung des Begrenzu durch Nutzer (für den Auftragsverarbeiter)

Säule 3: Datenminimierung

Verarbeitung muss auf ein Minimum an pbD beschränkt werden, d.h. bei der Auswahl der zu erhebenden pbD müssen die folgenden Grundsätze beachtet werden:

1. Adäquat (zu Verwendungszweck(en)): z.B. durch Vermeidung überflüssiger Daten.
2. Relevant: z.B. durch Vermeidung unnötiger Details
3. Eingeschränkt: in Bezug aus (Mindest-)Aufbewahrungsfrist.
4. Einsatz von Minimierungstechniken wie Anonymisierung oder Pseudonymisierung
5. Prozessdesign zur Minimierung

≠

Säule 4: Richtigkeit

Persönliche Daten müssen korrekt aufbewahrt werden:

Für den Sachbearbeiter/Verarbeiter

1. Überprüfung der Richtigkeit und Aktualität der pbD
2. Schneller Prozess zur Korrektur oder Zerstörung ungenauer pbD

Für den IT-Lösungsanbieter (Service, Software oder System)

1. Prozessdesign zur Sicherstellung der pbD-Genauigkeit
2. Merkmale des Verarbeitungsprozesses zur Korrektur oder Löschung fehlerhafter pbD.
3. Verarbeitungsprozesseigenschaften zur Sicherstellung der pbD-Genauigkeit.
4. Informationen und Verhaltenskodex zur Förderung der Anwendung des Prinzips der Begrenzung von pbD pro Nutzer

Säule 5: Konservierung

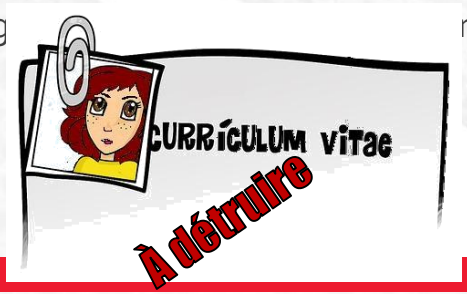
Personenbezogene Daten sollten nur dann gespeichert werden, wenn dies für den Zweck der Verarbeitung erforderlich ist:

Für Verantwortliche

1. Verarbeitung, die es unmöglich macht, die natürliche Person über den Zweck der Verarbeitung hinaus zu identifizieren.
2. Im Übrigen erfolgt die Verarbeitung ausschließlich zu Archivierungszwecken von öffentlichem Interesse oder für wissenschaftliche, historische oder statistische Zwecke.

Für pbD-Auftragsverarbeiter

1. Prozessdesign zur Sicherstellung der Begrenzung der pbD-Speicherung
2. Merkmale des Verarbeitungsprozesses zur Sicherstellung der Speicherbegrenzung von pbD.
3. Informationen u… örderung der Anwendung …rbegrenzung von pbD durch …



Säule 6: Vertraulichkeit und Datenintegrität

pbD müssen vertraulich und unverfälscht behandelt werden.

Für Verantwortliche und pbD-Auftragsverarbeiter

1. Die bei der Verarbeitung angewendeten (technischen und organisatorischen) Sicherheitsmaßnahmen sind ausreichend,
   1. um den Schutz der pbD vor unbefugter oder illegaler Verwendung zu gewährleisten,
   2. um den Schutz der pbD vor Zerstörung oder Korruption zu gewährleisten

Für den IT-Lösungsanbieter (Service, Software oder System)

1. Prozessentwurf
2. Funktionalität
3. Informationen und Verhaltenskodex für Daten und IT-Benutzer

zur Gewährleistung der Vertraulichkeit und Integrität von pbD.

Säule 7: Verantwortlichkeit

Der Verantwortliche (und ggf. pbD-Auftragsverarbeiter) müssen Rechenschaft, über die Einhaltung des DV-GVO ablegen können (insbesondere bei einem Vorfall).

Für Verantwortliche

1. Umsetzung von Sicherheitsmaßnahmen (technisch und organisatoris
   Nachweis der Einhaltung der wesentlichen Grundsätze der DGMP
2. Sicherheitsmaßnahmen (technisch und organisatorisch) werden regel
   überprüft und aktualisiert (Effektivität).

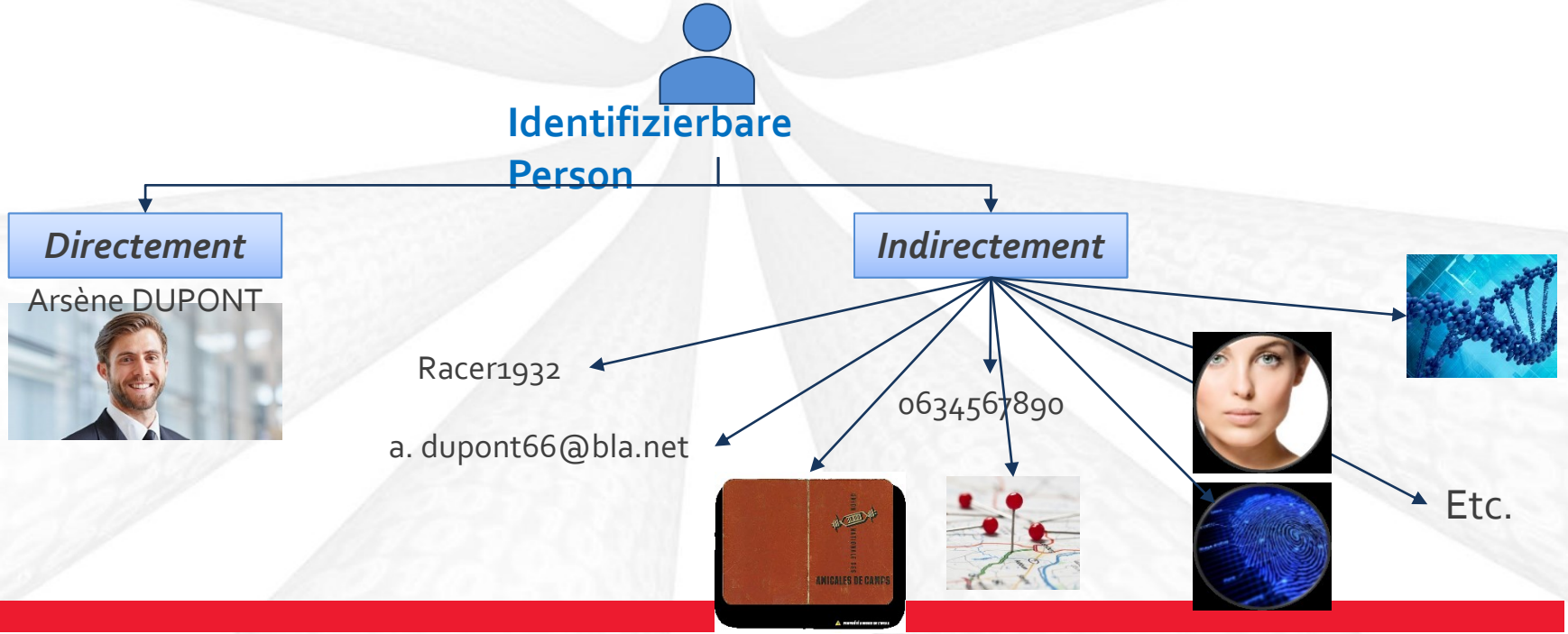
Für den IT-Lösungsanbieter (Service, Software oder System)

1. Die Prozessgestaltung demonstriert die Einhaltung der Grundprinzipi
   DGMP.
2. Die Merkmale des Verarbeitungsprozesses zeigen die Einhaltung der Grundprinzipien der DGMP.
3. Informationen und Verhaltenskodex, um sicherzustellen, dass die Verwendung der Verarbeitung es ermöglicht, diese Verantwortungspflicht zu gewährleisten.

pbD: kleine Erinnerung

Was sind personenbezogene Daten?

Artikel 4: *"Persönliche Daten" sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person.*



Fallstudie: Identifizierung persönlicher Daten

Alle diese Daten sind charakteristisch für eine natürliche Person….

- Geburtsjahr: 1966
- Geburtsdatum und -ort: 23/06/2008 + Luxemburg
- Geburtsdatum und Geschlecht: 14/05/2010 + Clervaux +
- Zeit, Datum, Geburtsort und Geschlecht: 23/06/2008 + Luxemburg + 02:40
- Zufälliger/regelmäßiger Standort
- Mac-Adresse

Identifizierbare Person

… aber nicht alles identifiziert die physische Person

Kategorie der pbD

Allgemeine Daten

- Informationen über die natürliche Person: Name, Vorname korreliert mit der Telefonnummer, Familienstand, Identität, Identifikationsdaten, E-Mail-Adresse usw. Persönliches Leben (Lebensstil, Hobbys, Familiensituation usw.).
- Identifizierung der juristischen Person, wenn es möglich ist, eine natürliche Person zu identifizieren.
- Informationen über die berufliche Tätigkeit: Wirtschafts- und Finanzinformationen (Einkommen, Finanzlage, Steuersituation usw.), Informationen über die Arbeitsbedingungen usw.
- Arbeitszeit (Beginn/Ende/Pause) bezogen auf die natürliche Person
- Digitale Fingerabdrücke
- Das von einer Kamera aufgenommene Bild einer Person
- Dynamische IP-Adresse
- Cookies, wenn sie eine eindeutige Kennung der natürlichen Person enthalten
- Lokalisierungsinformationen (Reiserouten, GPS Daten, GSM, etc.)
- IP-Standortdaten (Wi-Fi korreliert mit eindeutiger Mac-Adresse)
- Verbindungsdaten (IP-Adresse, Protokolle, etc.)
- RFID-Information, wenn sie die natürliche Person eindeutig identifiziert

Kategorie der pbD

Sensible Daten (Art. 9.1)

- Ethnische oder rassische Herkunft
- Politische Ansichten
- Philosophische oder religiöse Überzeugungen
- Gewerkschaftsmitgliedschaft
- Genetische Informationen
- Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Informationen zu Gesundheitsdaten
- Informationen über Sexualleben oder sexuelle Orientierung
- Eindeutige nationale Identifikationsnummer (Personalnummer)

Personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten (Art. 10)

- Erfasste Daten zu Straftaten
- Strafregister

Datenkategorie (Klassifikation nach CNPD)

Das CNPD bezieht sich in seinem Tool auf folgende Klassifikation der Daten

A: Nationale Identifikationsdaten

B: Données bancaires et financières autres que celles sujettes aux „Verarbeitung" concernant le crédit et la solvabilité des personnes

C: Caractéristiques personnelles autres que celles sujettes aux „Verarbeitung" qui révèlent l'Ethnische oder rassische Herkunft les Politische Ansichten, les convictions religieuses ou philosophiques, l'Gewerkschaftsmitgliedschaft, ainsi que les „Verarbeitung" de données relatives à la santé et à la vie sexuelle, y compris le „Verarbeitung" des données génétiques

D:Données physiques

E: Habitudes de vie et de consommation autres que celles sujettes aux „Verarbeitung" relatifs à la vie sexuelle

F: Données psychiques autres que celles sujettes aux „Verarbeitung" relatifs à la santé

G: Composition du ménage

H: Loisirs et intérêts

I: Affiliations et situation de membres

K: Biens et services fournis et reçus

L: Caractéristiques du logement

M: Données relatives à la santé pour les traitements mis en œuvre par les établissements hospitaliers et les médecins traitants et ceux nécessaires à la sauvegarde des intérêts vitaux d'une personne incapable de donner son consentement (art.6 et 7 de la loi)

N: Éducation, formation et qualification

O: Profession et emploi – Salaire – Évaluation - Sécurité

P: Données judiciaires sujettes aux traitements visés à l'article 8 de la loi

Q: Données raciales ou ethniques sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (c) de la loi Q.

R: Données relatives au comportement sexuel sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (c) de la loi

S: Opinions politiques aux traitements visés à l'article 6 paragraphe 2 lettre (d) de la loi

T: Affiliation syndicale sujette aux „Verarbeitung" visés à l'article 6 paragraphe 2 lettre (d) de la loi

U : Convictions philosophiques ou religieuses sujettes aux traitements visés à l'article 6 paragraphe 2 lettre (d) de la loi

V: Enregistrement d'images

W: Enregistrements de sons

Einwilligung

Einwilligung: Erinnerung

Wann ist für die Verarbeitung keine Einwilligung erforderlich?

Immer dann, wenn die Verarbeitung auf einem anderen Rechtsgrund beruht:

Vertragserfüllung

Wahrung lebenswichtiger Interessen

Gesetzliche Verpflichtung

Öffentliches Interesse

Interessenausgleich (*intérêt légitime*)*)*

Einwilligung

Art« . 4.11 *"Einwilligung der bPerson bedeutet jede freie, spezifische, informierte und eindeutige Manifestation von volonté, mit der die bPerson durch eine klare Erklärung oder positive Handlung akzeptiert, dass sie betreffende personenbezogene Daten verarbeitet werden dürfen".*

Freiwillig gegeben

Eindeutige Anzeige der kzeptanz

Spezifisch

Informiert

Zustimmung (Bemerkung WG Art29: 17/EN/259)

Frei / frei gegeben: impliziert eine echte Wahl und unter der Kontrolle des Subjekts.

1. Die Auswahl darf auf keinen Fall durch den Prozessor eingeschränkt werden (insbesondere im Falle einer unausgewogenen Beziehung).).
2. Im Falle der Erbringung einer Dienstleistung darf die Einwilligung nur die für die Vertragserfüllung unbedingt erforderlichen Daten umfassen.
3. Im Falle eines Vertrags: Es ist wichtig, den Umfang des Vertrags zu bewerten auch wenn in diesem Fall die Zustimmung implizit im Vertrag enthalten ist.

Ein Vertrag kann unter keinen Umständen die Rechtsgrundlage für die Verarbeitung sensibler Daten sein.

Zustimmung (Bemerkung WG Art29: 17/EN/259)

Frei / freiwillig gegeben:

4. nicht generell, sondern für alle Behandlungen einzeln.
5. Der Verarbeiter muss nachweisen können, dass die Zustimmung jederzeit ohne finanziellen Nachteil verweigert werden kann.

Zustimmung (Bemerkung WG Art29: 17/EN/259)

Spezifisch/Endpunkt(e): klar sein

1. Geben Sie die Zwecke an.
2. Sicherstellung der Möglichkeit einer granularen Einwilligung
3. Trennung zwischen Informationen über die Einwilligung in die Verarbeitung und anderen Informationen (insbesondere vertraglichen Informationen) sicherstellen.

Zustimmung (Bemerkung WG Art29: 17/EN/259)

Informiert: Die Einwilligung muss auf der Grundlage des Wissens des Nutzers erfolgen, ansonsten keine Einwilligung..

Minimale Informationsspezifikation.

a) Identität der Verantwortlichen
b) Zweck eines jeden Verarbeitungsvorgangs
c) Art der gesammelten Daten
d) Bestehen eines Widerrufsrechts
e) Informationen bei automatisierten Entscheidungen
f) Informationen, wenn die Einwilligung die Übermittlung von Daten in ein Drittland umfasst.

Zustimmung (Bemerkung WG Art29: 17/EN/259)

Informiert:

1. Mittel zur Informationsübermittlung: keine Medientypverpflichtung
2. Konzentration auf das Verständnis der Einwilligung

Eindeutig:

1. Die Einwilligung muss in einem aktiven Prozess formalisiert werden: bewus
   Handlung (die Verwendung von vorab angekreuzten Kästchen ist verboten)
2. Bei elektronischen Systemen: Die Aktion kann eine physische Geste sein.
3. Das Einwilligungsverfahren muss eine Ermüdung oder Ermüdung des Benutzers vermeiden.

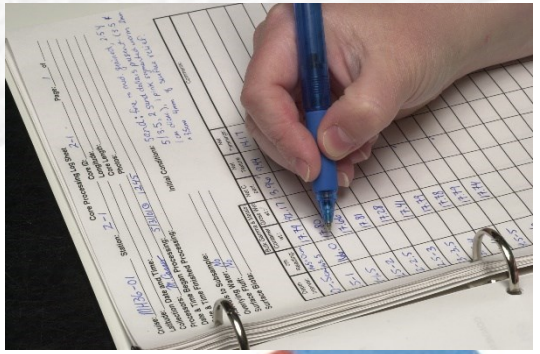
Zustimmung (Bemerkung WG Art29: 17/EN/259)

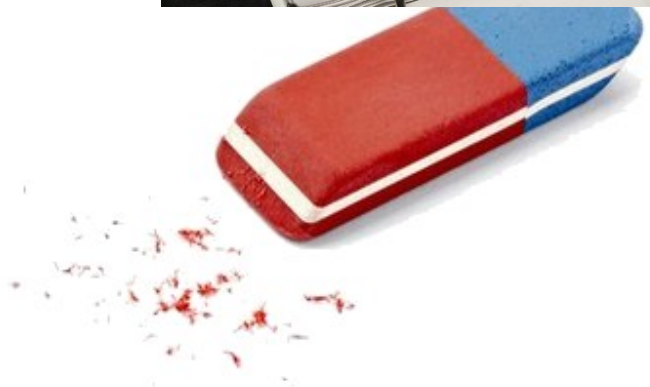
Explizite Einwilligung: in einigen Fällen (**sensible Daten**))

1. Der Benutzer gibt eine formelle Erklärung ab (z.B. schriftlich).
2. Dies bedeutet nicht Papier: elektronisches Formular, E-Mail oder zweistufiger Prozess (Antwort erforderlich mit "Ich stimme zu")

Zusätzliche Gültigkeitsbedingungen::

1. Verpflichtung des Verantwortlichen zum Nachweis der Einv Nutzers
2. Verpflichtung zum Widerruf der Einwilligung
3. Hinweis: Zeitliche Begrenzung: keine a priori-Beschränkung, es sei denn, es fin der Behandlung statt. Gute Praxis: Fragen Sie in regelmäßigen Abständen nach





Einwilligung: kommerzielle Informationen und Werbung

1. Verpflichtung zur Einholung der Einwilligung vor jeder Behandlung (OPT-IN) für
    1. elektronische Aufforderung (sms, mail, mms)
    2. Übertragung oder Austausch von elektronischen Kontaktinformationen zu diesem Zweck
2. Ausnahmen:
    1. Versand an Geschäftsadresse und Geschäftsgegenstand
    2. Nachricht für identische Produkte oder Dienstleistungen
3. Verpflichtung zur Einhaltung:
    1. das Widerspruchsrecht (einfach und kostenlos)
    2. Begrenzung der Vorratsdatenspeicherung (z.B. <3 Jahre ohne Antwort des Betroffenen)
    3. Sicherstellen, dass die Daten nicht für andere Zwecke verwendet werden können (Vertragsklausel bei Verwendung eines Dienstleisters).)
4. Verbot:
    1. Informationen auf Websites oder Foren sammeln
    2. vermutete Einwilligung (Prüfung vorgefüllt)
    3. den Zugang zu einer Dienstleistung von der Annahme des Antrags abhängig machen.
5. Nutzung öffentlicher Unternehmensverzeichnisse: möglich

Einwilligung: Wie geht es weiter?

1. Keine Regeln für die zu informierenden Medien:
   - In schriftlicher oder mündlicher Form
   - Papier, Elektronik
   - Audiobotschaft, Video, etc.
2. Das Wichtigste: **Sammeln** Sie einen eindeutigen Hinweis auf die Wahl: **klare bejahende Massnahmen**die nicht an die Annahme eines Vertrages oder die Bedingungen einer Dienstleistung gebunden sind, etc.
3. **Nachweis** der Einwilligung.

Praktisch:

- Erfassung formaler Antworten (z.B. auf die Annahme einer Datenschutzerklärung): Mail-Antwort auf eine formelle Anfrage
- Akzeptanz über ein Formular einholen (Eindeutigkeit der Informationen)

Einwilligung: Behandlungen nach RL 95/46/EG

Laufende Verarbeitungen, die rechtmäßig sind und auf einer Einwilligung beruhen, erfordern nicht zwingend eine erneute Einwilligung wegen DS-GVO.

- Die Einwilligung wurde protokolliert.
- Es gibt ein Verfahren für den Widerruf der Einwilligung (einschließlich der Granularität).

Und wenn die Einwilligung nicht konsistent ist, vor 25. Mai:

1. bitten Sie erneut um Zustimmung,
2. beurteilen Sie, ob die Verarbeitung auf einer anderen Rechtsgrundlage beruhen kann,
3. oder Beenden Sie die Behandlung.

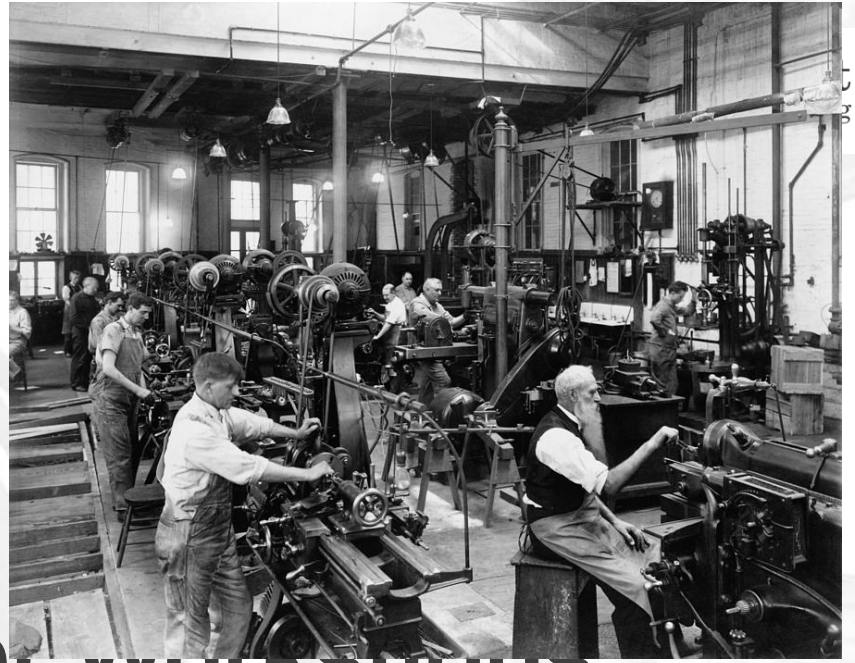
Mit richtigen Reflexen zur Konformität

Wichtige Punkte, die es zu beachten gilt

- eine **Bestandsaufnahme** der Verarbeitungstätigkeiten und ihrer primäre und sekundäre Zwecke sowie der Rechtmäßigkeit der einzelnen Verarbeitungsvorgänge vorzuneh
- Identifizieren Sie für **jeden Verarbeitungsvorgang** den Controller und **ggf.** die und den DPO.
- Bestimmen **Sie die Art** der verarbeiteten Daten und überprüfen Sie, ob sie ordr verwendet werden: in Verbindung mit dem Zweck und in angemessener Weise (Minimierung
- Überprüfen Sie, ob für jede Daten (oder Datengruppe) **ein Aufbewahrungsdatu** wurde und ob ein sicherer Vernichtungsprozess vorhanden ist.
- Überprüfen, ob **Sicherheitsmaßnahmen definiert wurden,** um den Schutz de Weiterverfolgung ihres Zugriffs und die Kontrolle dieser Maßnahmen (Anwendu zu gewährleisten.
- Identifizieren **Sie den** Datenaustausch (intern/extern), um Verstöße zu verr sicherzustellen, dass ein solcher Datenaustausch möglich ist (rechtlich und schützend).

Zu schreibende Dokumente

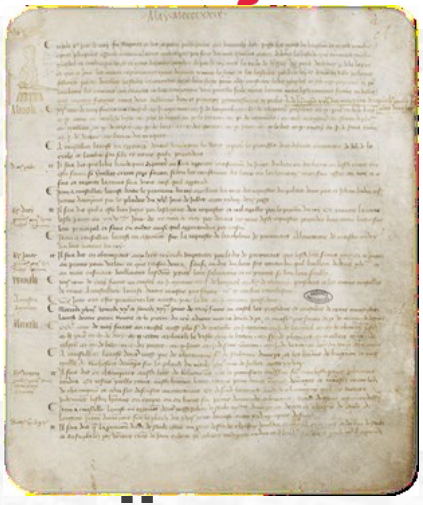
- **Register der Verarbeitungsvorgänge** (obligatorisch): ersetzt die Meldung an die CNPD für viele Verarbeitungsvorgänge.
- **Datenschutzerklärung(en)**: für den internen und externen Gebrauch
- **Verhaltenskodex für Daten und IT-Benutzer**
- Vertragsklausel in Verträgen mit pbD-Auftragsverarbeitern zur Sicherstellung der Einhaltung des DS-GVO
- **Verfahren bei Verletzung des Schutzes** (Meldung an CPND und/oder pPerson)
- Verfahren zur Datenportierung
- Sicherheitsüberwachungs- und Kontrollverfahren zum Schutz pdD
- Datenschutz-Folgenabschätzung (bei hohem Risiko)



Präsentation der Workshops

Plan der Präsentation der einzelnen Workshops

1. Bezug zu Anforderungen
2. Präsentation der Dokumente
3. Vorbereitung
4. Inhalt

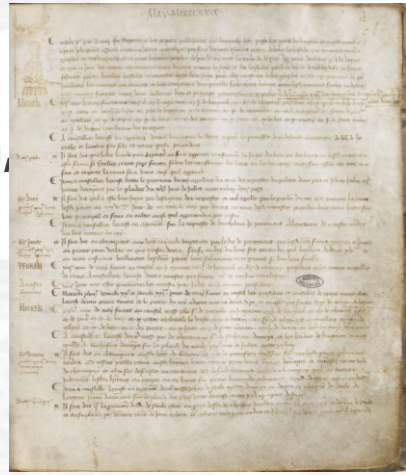


Register der Verarbeitungsvorgänge

Workshop: Register der Verarbeitungsvorgänge

Einrichtung eines Registers der Verarbeitungsvorgänge und einer Verpflichtung für den Kontrolleur und die Verarbeiter (Art. 30-1 und 30-2).

Sie ersetzt die bisherigen Meldungen von Verarbeitungsvorgängen an das NCDP.



Ausnahme: für KMU mit weniger als 250 Mitarbeitern, außer wenn eine der folgenden Bedingungen erfüllt ist:

1. bei Risiko für die Rechte und Freiheiten der pPerson
2. Verarbeitung nicht nur gelegentlich, ODER
3. Sensitive Daten nach Art. 9 und 10 betroffen sind.

Praktisch: Es ist ratsam, dieses Register in allen Fällen einzurichten,

Das die mind. eine Verarbeitung i.a. regelmäßig ist.

Workshop: Register der Verarbeitungsvorgänge

Inhalt (für den Verantwortlichen)?

a) Name und Kontaktdaten des Verantwortlichen. (evtl. Name des Vorgesetzten und DSB)
b) Zwecke der Verarbeitung
c) Beschreibung Datenkategorie
d) Empfänger-Kategorie
e) Datenübermittlung an Drittstaaten und internationale Organisationen
f) Soweit möglich: Fristen für die Löschung von pbD
g) Soweit möglich: Soweit möglich: Allgemeine Beschreibung der Sicherheitsmaßnahmen, ...

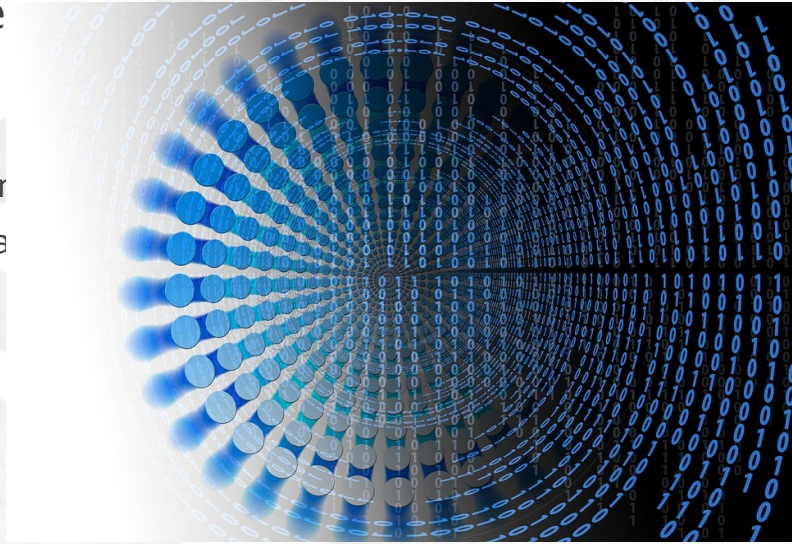
Inhalt (für den pbD-Auftragsverarbeiter)?

a) Name und Kontaktdaten des pbD-Auftragsverarbeiter und jedes Verantwortlichen, für den der pb Auftragsverarbeiter tätig ist. (evtl. Name des Vorgesetzten und DSB)
b) Beschreibung Datenkategorie
c) Datenübermittlung an Drittstaaten und internationale Organisationen
d) Soweit möglich: Soweit möglich: Allgemeine Beschreibung der Sicherheitsmaßnahmen, ...

Workshop: Register der Verarbeitungsvorgänge

Typische Verarbeitungen für das Verarbeitungsregiste

- Personalaktenverwaltung und Lebensläufe von Bewerbern
- Gehaltszahlungen
- Rechnungs- und Angebotsmanagement für Kunden und Lieferar
- Management der Nutzung von IT-Ressourcen durch das Persona
- Verwaltung von Mitarbeiter-Geolokalisierung
- Verwaltung der Datenbank mit potentiellen Kunden, etc.



Praktisch:

Anzahl und Art der Verarbeitungen zu definieren,

Logisch Prozesse Gruppieren oder aufspalten.

Workshop: Register der Verarbeitungsvorgänge

Modell eines Verarbeitungsregisters (Excel-Modell) zur Kodierung aller Verarbeitungsvorgänge. Dieses Dokument enthält verschiedene Arbeitsblätter:

- Historie: um anzuzeigen, wie das Dokument verwaltet wird (Arbeitsgruppe Verteilerliste, Freigaben…)
- Struktur: Informationen zur Dokumentstruktur
- Organisationen: Allgemeine Informationen über die Verarbeitung und Verantwortlichkeiten innerhalb der Organisation in Bezug auf den Schutz personenbezogener Daten (pbD)
- Übersicht: Zusammenfassung wichtiger Informationen aus jeder Verarbeitung
- Register: Informationen zu den verschiedenen Verarbeitungen nach der DS-GVO
- Optional: allgemeine Maßnahmen: Checkliste der Sicherheitsmaßnahmen für alle Verarbeitungen, um den Schutz der pbD zu gewährleisten.
- Optional: Risiko max.: Tabelle zur Angabe des höchsten Risikos für jede Verarbeitung.
- Rechtmäßigkeit und Risikoskala: Informationstabellen mit Rechtsgrundlagen zur Rechtsmäßigkeit und die in der Risikoanalyse verwendeten Skalen.

Die mitgelieferte Vorlage ist für einige Standardverarbeitungen (generisch) vorausgefüllt.

Workshop: Register der Verarbeitungsvorgänge

Vorbereitung

- Anpassung bereits vorgefüllter Behandlungen an Ihr Unternehmen
- Identifizieren Sie, ob es in Ihrem Unternehmen noch andere Behandlungen gibt.
- Erstellen sie eine Spalte für jeden weitere Verarbeitung
- Notieren Sie sich alle auftretenden Fragen und leiten Sie sie an uns weiter (RGPD@itrust.lu).)

Inhalt

- Erklärung der einzelne Felder
- Diskussion des Zwecke, Entscheidungen…
- Case by Case Support

Datenschutzerklärung

Der Verantwortliche muss den betroffenen Personen die Ausübung ihrer Rechte ermöglichen und sie insbesondere darüber informieren. **(keine offizielle Anforderung)**

Wann? Im Allgemeinen zum Zeitpunkt der ersten Mitteilung. Aber es kommt darauf an, wie Sie die Daten sammeln.

In welcher Form? Um alle Informationspflichten der DS-GVO zu erfüllen, ist es oft sinnvoll, eine Datenschutzerklärung oder Vertraulichkeitspolitik zu erstellen.

- Lange Version (wird zuerst erstellt)
- Kurze Version (mit Bezügen auf das lange Modell) mit den Schlüsselelementen, für Einholung der Einwilligung.

Wann nachbessern? Sobald sich die Verarbeitungsmethoden ändern: neue Zwecke, neue pbD-Auftragsverarbeiter, größere Veränderungen (Übermittlung, Profiling)

Workshop: Datenschutzerklärung

Eine Datenschutzerklärung sollte sich an eine Gruppe von Empfängern richten und in der Regel folgende Elemente enthalten

- Grundsatzerklärung unter Hinweis darauf, dass die Organisation bei der Verarbeitung pbD die Menschen und ihre Rechte berücksichtigt.
- Verhaltensregeln für die Verarbeitung (mit dem Datum der letzten Aktualisierung)
  - Verpflichtung des Verantwortlichen
  - Geltungsbereich dieser Regeln (Zweck(e) der Verarbeitung, einschließlich Sekundärverarbeitung)
  - Verantwortung (inkl. DPO) mit Kontaktdaten
  - Umsetzung der Einwilligung
  - Welche Daten und wie erhoben?
  - Verwendung
  - Datenempfänger (Sharing und Kommunikation)
  - Datenübernahme
  - Schutz der Daten
  - Rechte der bPersonen und Ausübung?
  - Änderungsmöglichkeiten

Möglicherweise

- Möglicherweise
  - Cookie (Website)
  - Google Analytics-Dienst
  - Für kommerzielle Zwecke

Workshop: Datenschutzerklärung

Datenschutzerklärungsvorlage: Für den Workshop zum Thema Datenschutz stehen Ihnen 3 Dokumente zur Verfügung

1. Ein Leitfaden zum Schreiben
2. Ein Muster für Ihre Mitarbeiter
3. Eine lange Vorlage von Anweisungen an Ihre Kunden, pbD-Auftragsverarbeiter, Website-Besucher….

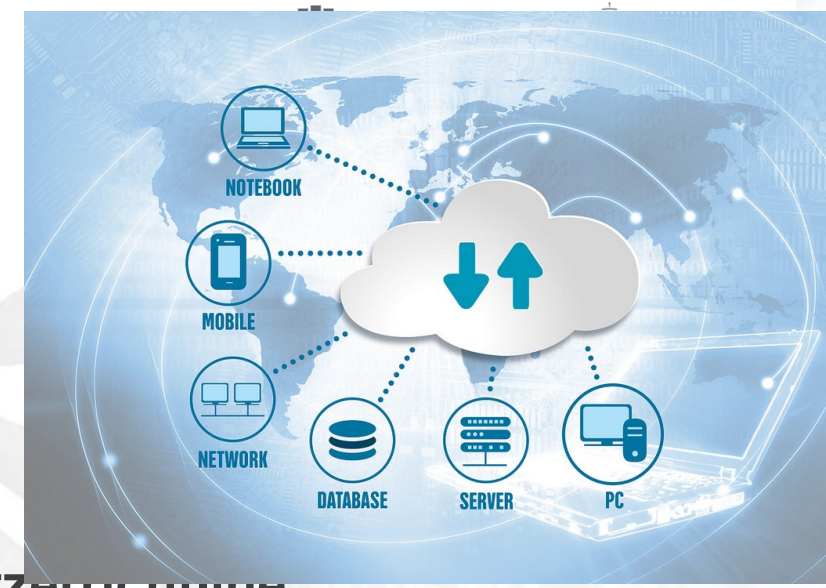
Workshop: Datenschutzerklärung

Vorbereitung

- Passen Sie die Datensätze an oder schreiben Sie sie für Ihr Unternehmen.
- Fragen aufschreiben (oder an RGPD@itrust.lu weiterleiten)

Inhalt

- Antworten.
  - Einordnung des Themas in den Regelungsrahmen
  - Vorschläge einer oder mehrerer Lösungen
- Diskussion
- Case by Case Support.
- zusätzliche Fragen oder Beispiele.



Daten und IT-Benutzerrichtlinie

Wichtige Sicherheitsprinzipien in der DS-GVO:

- Verantwortlichkeit und Verantwortung

Art. 24.1 *"Unter Berücksichtigung von Art, Umfang, Kontext und Zweck der Verarbeitung sowie der Risiken*, einschliesslich degré *von probabilité und gravité, für die Rechte und Freiheiten natürlicher Personen, hat der für die Verarbeitung Verantwortliche geeignete* ***technische und organisatorische Maßnahmen zu treffen, um sicherzustellen und nachweisen zu können, dass die Verarbeitung effectué in Übereinstimmung mit diesen Vorschriften erfolgt.*** *Diese Maßnahmen werden überprüft und gegebenenfalls aktualisiert..* »

- Verpflichtung zur konsequenten und zielgerichteten Umsetzung von Maßnahmen

Art. 32.1 ***"Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos*** *für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter* ***geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten….***".

Art. 32.2 *"Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu pbD, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.".*

Workshop: Verhaltenskodex für Daten und IT-Benutzer

Ein einfacher Weg, die Sicherheit zu organisieren, ist die Umsetzung einer Charta oder Richtline, um der richtige Verhalten der Benutzer im Bereich der Informationssicherheit sicherzustellen.

Zweck:

- Informieren Sie alle Benutzer über ihre Rollen und Verantwortlichkeiten bei der Nutzung der Computersysteme (und Daten!) ihres Unternehmens, auch im Hinblick auf ihre Verantwortung für den Datenschutz.
- Ihre Einwilligung

Inhalt:

1. Grundsätze für den Schutz pbD
2. Unternehmensethik
3. Die Bedeutung jedes einzelnen im Risikomanagement
4. Die Bedeutung jedes einzelnen bei Vorfällen und Verstößen
5. Die Umsetzung einer Sicherheitspolitik im Unternehmen
6. Praktische Regeln für die Umsetzung der Sicherheit: für Telearbeit, Clean-Desk-Politik usw.

Workshop: Verhaltenskodex für Daten und IT-Benutzer

Inhalt:

6. Die Bedeutung des Faktors Mensch (Personalsicherheit, Fehler im Umgang mit Informationen)
7. Die Bedeutung eines sorgfältigen Asset Management (Datenklassifizierung/Nutzung und Unterstützung)
8. Die Regeln für den (physischen und logischen) Zugriff auf Informationen
9. Die Verwendung von Verschlüsselungsmitteln
10. Spezifische Regeln für die Nutzung von Computerressourcen (PC, Handy, Tablet, Netzwerke, etc.)
11. Störungsmanagement….
12. Compliance Management Maßnahmen: Systemüberwachung, Sanktionen, etc.

Workshop: Verhaltenskodex für Daten und IT-Benutzer

Was Sie vor dem Workshop zur Charta des guten Verhaltens tun sollten

- Passen Sie die Charta für Ihr Unternehmen an oder schreiben Sie sie auf der Grundlage des Modells.
- Notieren Sie sich alle auftretenden Fragen und leiten Sie sie an uns weiter (DS-GVO@itrust.lu).

Was werden wir während des Good Conduct Charter Workshops tun?

- Wir kümmern uns um alle Fragen, die wir erhalten, um Ihnen bei der Fertigstellung Ihrer Unterlagen zu helfen.
  - Einordnung der Fragen in den Grundverordnungsrahmen
  - durch den Vorschlag einer oder mehrerer Lösungen
- Wir führen Sie während des Workshops durch die individuelle Erfassung Ihrer Charta (fallweise Unterstützung).
- Wir beantworten zusätzliche Fragen oder leiten Überlegungen anhand von Beispielen ein.

Einwilligung

Workshop: Einwilligung

Vorbereitung

- Identifizieren Sie Behandlungen, die auf einer Einwilligung beruhen (oder beruhen sollten).
- Vergewissern Sie sich, dass diese Einwilligung von der Person erteilt wurde und in den Geltungsbereich des Merkblatts aufgenommen wurde, und wenn nicht, schließen Sie sie ein.
- Vorbereitung der Methode zur Einholung und Aufhebung der Einwilligung (auch in Form von Informationen in Form einer E-Mail, eines Hinweises auf der Website oder auf Serviceverträgen etc.
- Passen Sie die Datensätze an oder schreiben Sie sie für Ihr Unternehmen.)

Inhalt des Workshops

- Neben der Erstausbildung stellen wir Ihnen Beispiele (korrekt oder nicht) des Einwilligungs- und Einwilligungsmanagements zur Verfügung, um das Training mit Beispielen zu vertiefen.
- Wir werden uns mit allen eingegangenen Fragen befassen, um entweder den Wortlaut oder die Mittel zur Verwaltung der Zustimmung zu verbessern.
- Wir beantworten zusätzliche Fragen oder leiten Überlegungen anhand von Beispielen ein.

Verbesserung der Compliance: zusätzliche Workshops

Weitere mögliche Workshops

Zusätzlich zu den bereits geplanten Workshops (und je nach Bedarf, Interesse und Anmeldung) **kann die** FdA in Zusammenarbeit mit itrust consulting 4 weitere Workshops organisieren:

- **Management und Benachrichtigung bei Sicherheitsverletzungen:** Umsetzung folgender Verpflichtungen

Art 33-1: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Art. 33-2: Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

- **Management von Auftragsverarbeitern und Vertragsklauseln**

Art. 28-1: Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Art 28-2: Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

- **Datenklassifizierung und verwandte Verfahren:** denn der Schutz personenbezogener Daten bedeutet vor allem, dass man sie identifizieren und verwalten kann.
- **Dokumentenmanagement:** Die DS-GVO veranlasst die Implementierung von Dokumenten, die es zu verwalten gilt: Aktualisierung, Verteilung, etc.

Fragen?

Kontaktinfo:
Carlo Harpes : harpes@itrust.lu
Ingo Senft: senft@itrust.lu

Danke für Ihre Aufmerksamkeit

Kontaktinfo:
Carlo Harpes : harpes@itrust.lu
Ingo Senft: senft@itrust.lu