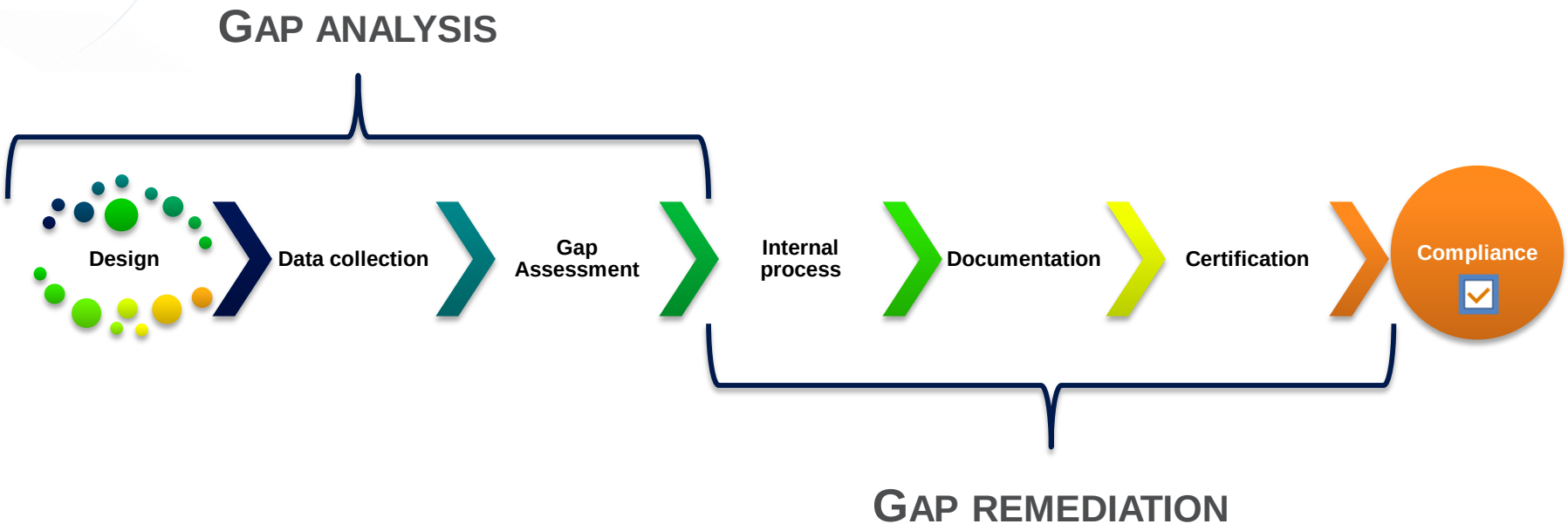
10 tips to assure more rapidly your GDPR compliance

Vincent Wellens

A steep road to data protection compliance…



Gap analysis…

Governance measures

Processing based analysis

Information security

Design

CNPD

GDPR Compliance Support Tool

Analysis

Lawful basis

Qualification controller / processor

Gap Assessment

Peripheral legislation

Data collection

Type of data

Record

1. Combine general governance / individual processing

Horizontal governance

- **General organisation**: was generally lacking → accountability!
- **Security measures**: synergies with general information security!
- **Processor relations**: often horizontal aspects (but not always)

Intermediary split into business divisions

- Sales
- HR
- Procurement,
- Corporate…

Individual processing activities

- Existing
+
- Future

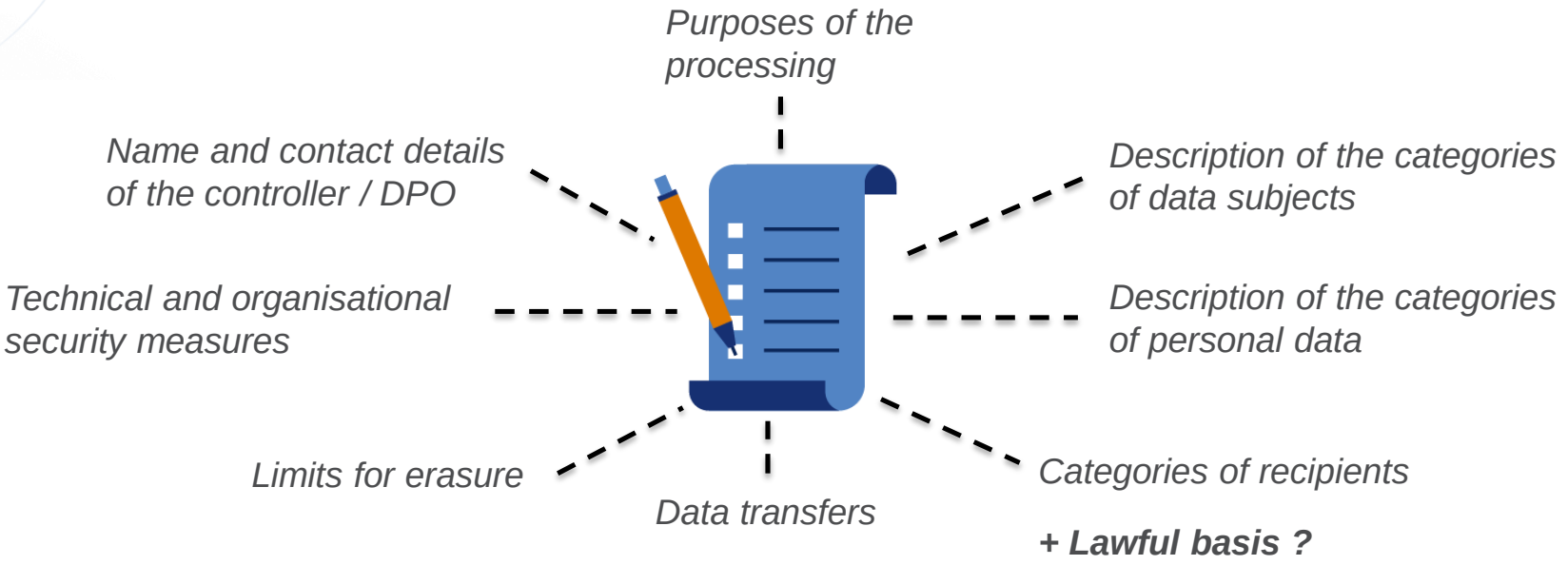
Top down approach:

without a sound general organisation, compliance downstream cannot be assured

IT needs to assist the whole top down process

2. Use the obligatory record as a basis for the gap analysis data mapping

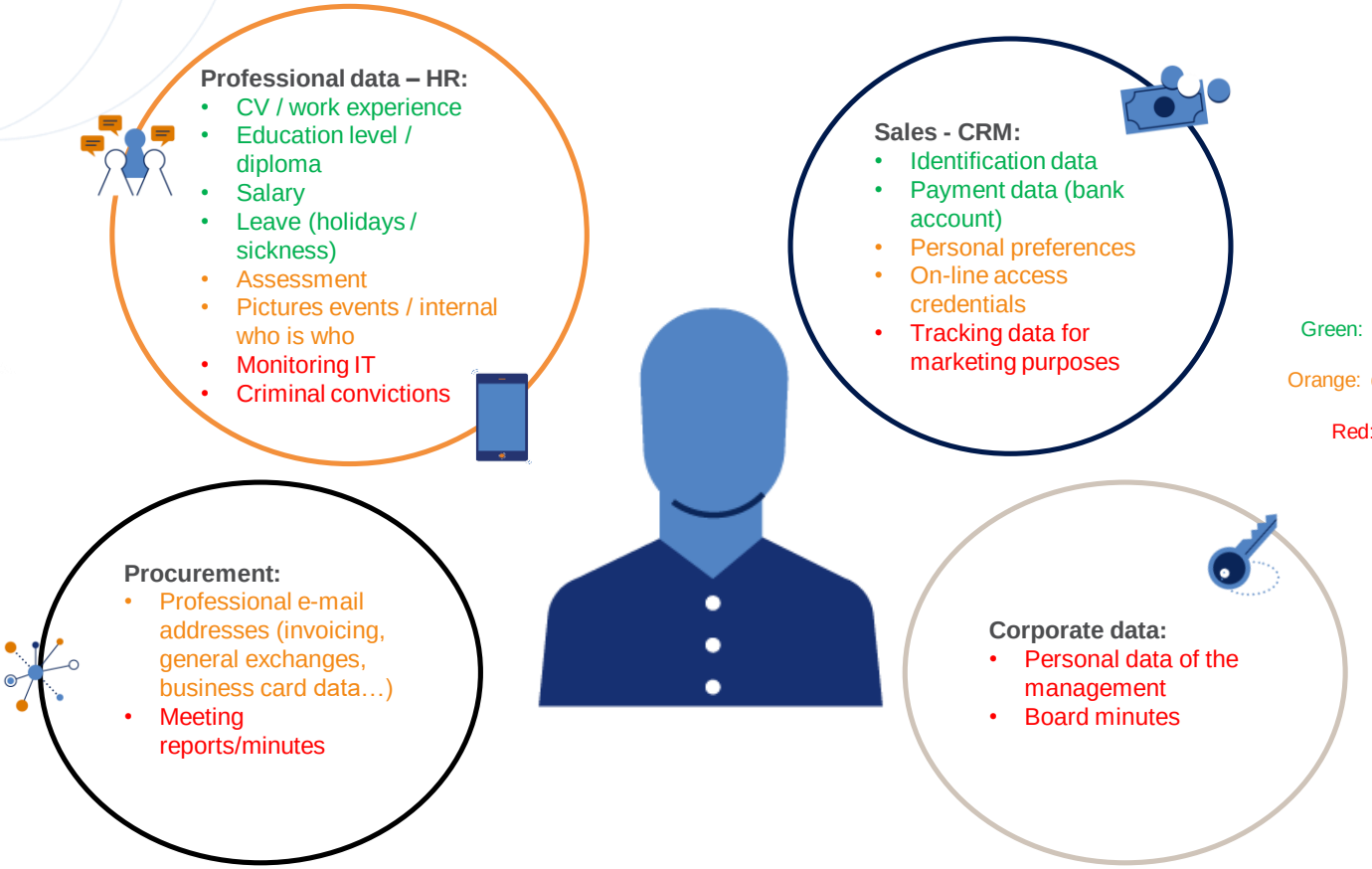
Art. 30 GDPR imposes the keeping of a record with all processing activities: **use it when collecting the data** at an individual processing level:



→ This excludes the IT approach to map data (but an IT based mapping is needed for reconciliation)

→ This ensures accurate records and will avoid double work even if a regular review will be necessary

3. Include all relevant categories of personal data



Green: data in principle included

Orange: data sometimes included

Red: data generally forgotten

- Not always an easy task as the definition of “personal data” is – sometimes surprisingly – large!
- Problem: it does not necessarily concern documents in their entirety

4. Qualify correctly controller / processor (1)

Controller

Determines processing **purposes and means**

- Based on facts
- Defined by law
- Implicit competence

Bears full compliance burden

Processor

Processes personal data **on behalf** of the controller

- Documented instructions

Limited direct regulatory and civil liability…

(even when increased obligations under the contract with the controller)

Compulsory contract

4. Qualify controller / processor (2)

Trends

Parties think that they can contractually define the right qualification

- Depends on the reality – authority / judge have the last word

The other party thinks that it is better to take on the role of <u>controller</u>

- Often they contribute in the same processing and are joint controllers (and not individual successive controllers): a joint controllership agreement is needed
- Often problem that it is difficult for that other party to assure directly compliance towards the data subject

The other party thinks that it is better to take on the role of <u>processor</u>

- If not reflecting the actual situation, risk of requalification *a posteriori* + in case of processing beyond the controller's instructions, liability!

5. Choose the correct lawful basis

Legitimate interest

- Requires a balancing test which is (nearly) never carried out although the CNPD may (and lately does) require proof concerning such test

Consent

- Too often relied upon (e.g. direct marketing but > ePrivacy regulation)
- Sometimes "back-up basis"→ not a solution – authorities do not like multiple bases or switching between legal bases!
- Risk of withdrawal
- Risk of invalidity (if not freely given)

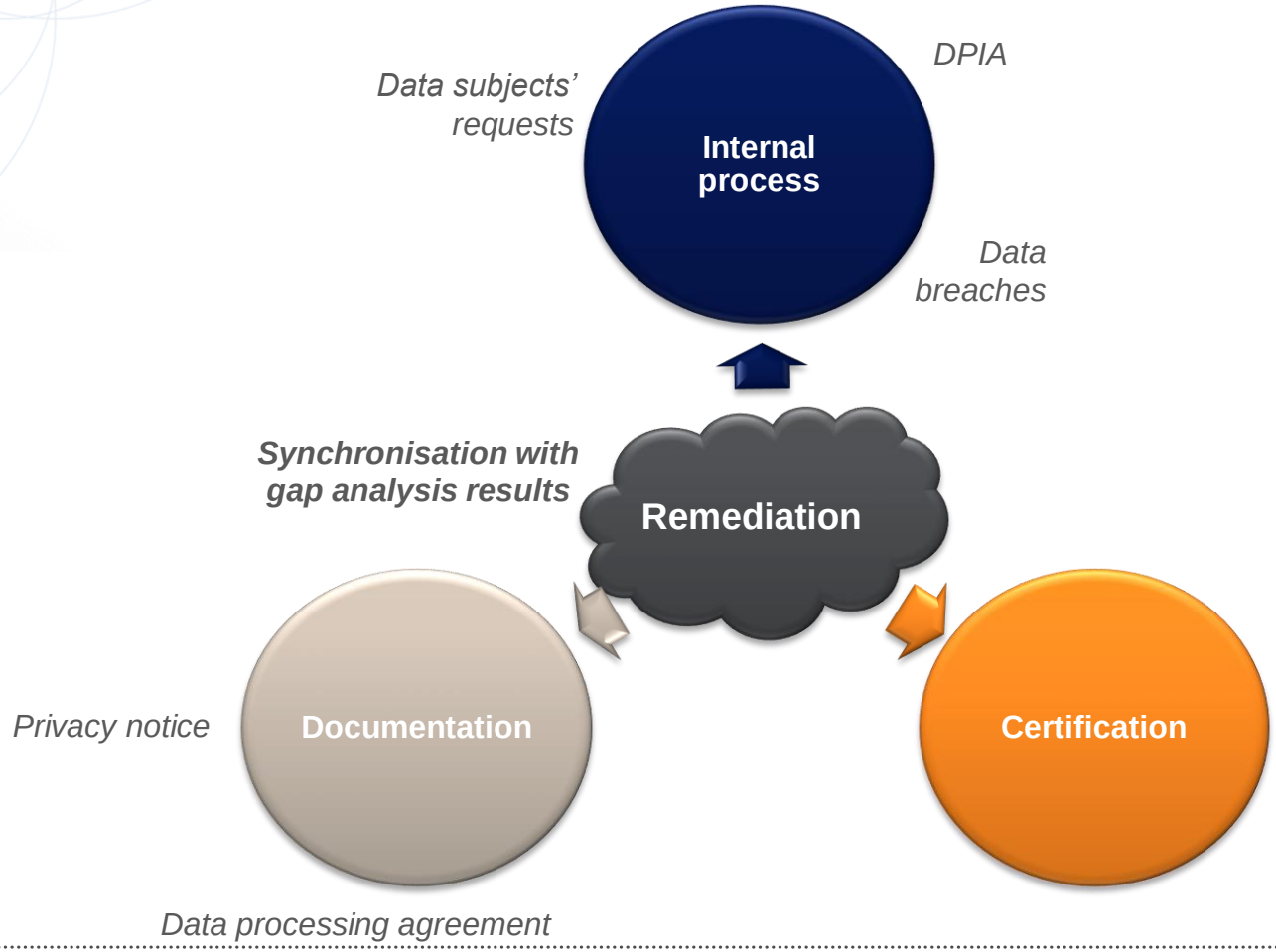
Legal obligation

- No sufficient knowledge about existing legal obligations
- Subtle but difficult difference between legal "obligation" and legal "permission" (→ legitimate interest)

It is key to take into account other applicable legislations

(retention obligations, employment law, image rights, e-privacy…)

Gap remediation…



6. Synchronise between gap analysis results and remediation documentation

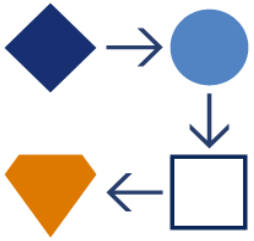
6	Gestion et suivi de la clientèle	Traitement de la clientèle sur la base des achats, des transactions commerciales ou autres relations professionnelles Suivi de la relation client (enquêtes de satisfaction, gestion des réclamations et service après vente) Elaboration de profil de la clientèle existante et la prospection de nouveaux clients	Les clients de l'organisation	Identification Identification électronique Données financières	Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci	10 ans	Gestion des accès sur le principe du "Need to know" Tenue d'un journal des accès aux dossiers Protection contre les logiciels malveillants Sécurité du périmètre réseau
7	Gestion des fournisseurs	Gestion et administration des fournisseurs et les commandes auprès fournisseurs	Fournisseurs en relation avec l'organisation	Identification Identification électronique Données financières	Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci	10 ans	Protection contre les logiciels malveillants
8	Marketing direct	Constitution d'un fichier client en vue d'une exploitation de marketing direct Envoi de newsletter	Clients de l'organisation Prospects	Identification Identification électronique Profession et emploi Caractéristiques personnelles Loisirs et intérêts	Consentement de la personne	Durée de la relation entre les personnes concernées et le responsable de traitement Retrait du consentement de la personne concernée	Gestion des accès sur le principe du "Need to know" Transferts sécurisés des données vers des tiers Minimisation des données transférées vers les sous-traitants Protection contre les logiciels malveillants Sécurité du périmètre réseau/Protection contre les intrusions (Firewall)
9	Gestion des cartes de fidélités des clients	Programme de fidélité destiné aux clients	Clients de l'organisation	Identification Caractéristiques personnelles Composition du ménage Habitudes de consommation	Consentement de la personne	Jusqu'à retrait du consentement de la personne Après 6 mois d'inactivité de la carte de fidélité Jusqu'à l'expiration de la carte de fidélité	Gestion des accès sur le principe du "Need to know" Anonymisation des données dès que possible pour effectuer des statistiques Protection contre les logiciels malveillants Sécurité du périmètre réseau/Protection contre les intrusions (Firewall)

Privacy notice
Consent

Contracts (DPAs, joint controllership…)

Record

DPIA



BCRs / SCC

6. Synchronise between gap analysis results and remediation documentation

KLM Privacy Policy

In this privacy policy we explain how we collect and use your personal information. This privacy policy applies to all personal information we process about you when you travel with us, purchase or use our services, visit our websites, use our mobile applications or otherwise interact with us. We have divided this privacy policy into different sections. Please click on the relevant section below for further information.

- 1. Who we are
- 2. The types of personal data we process
- 3. How we collect your data
- 4. For which purposes we use your data
- 5. Disclosing or sharing data with third parties
- 6. Security and retention
- 7. International transfer of your data
- 8. Your rights
- 9. How we look after this policy

2. The types of personal data we process

2.1 General. We may collect and process the following categories of personal information:

a. Name, passport number and other identifying information
For example, we may record your name, title, gender and date of birth, your nationality, country of residence and passport number.

b. Your contact details and personal account or registration details
Your contact details may include your address, telephone number and e-mail address. When you create a personal account, or register for a service, we may also record your sign in details and other information you fill out on your personal account or registration form. For business travellers, we also collect information relating to your company such as company name and business location.

c. Information about your reservations, bookings and purchases
When you make a reservation, or book a flight with us, we process your reservation and booking information. This information may include details about your flight, prices and the date of your reservation or booking. In addition, we process information in relation to ancillary services (such as upgrades and extra luggage) and products you purchase (for example via the KLM webshop).

d. Information about your travel arrangements
When you travel with us, we process information in relation to your journey. Such as your travel itinerary, (online) check-in, your (mobile) boarding pass and your travel companions. We may also record any specified medical needs or dietary requests you have and any additional assistance you require.

e. Your membership of our loyalty programmes, like Flying Blue and BlueBiz
When you become a member of our loyalty programmes, we process your membership number, balance, awards and benefits, type and level of membership and other information in relation to

f. Our communication with you
When you send us an e-mail or chat with us online or via social media, we register your communi
We also register your communication preferences. For example when you unsubscribe from one
or when you choose to receive your booking related communication (such as confirmation, check
boarding pass, flight status updates) via other channels than e-mail (such as WhatsApp, Mes
WeChat). When you call us, our customer support will register your questions or complaints in ou
may also record telephone calls for training purposes or to prevent or combat fraud.

g. Information we collect when you use our websites, apps and other digital media
• When you visit our websites, or use one of our mobile apps, we may register your IP address, br
operating system, referring website, web-browsing behavior and app use. We also collect informa
and similar technologies when you visit our websites or use our mobile apps. For more informatio
our cookie policy on the website or the mobile app you use. • We may receive an automatic notif
open our e-mails or click on a link in such e-mails.
• With your permission, we may also receive your location data.
• You can also agree to provide us with access to certain data stored on your mobile phone (such
contacts).

h. Information in relation to social media
Depending on your social network settings we may receive information from your social network
example, when you sign in for our services using a social network account, we may receive your s
profile including your contact details, interests and contacts. For more information on the person
receive from your social network provider and how to change your settings, please check the web
policy of your social network provider.

i. Information you choose to share with us
You may choose to share information with us, for example when you share your interests and pre
leave a comment for us on Facebook, fill out a customer survey or submit an entry for a contest.

4.1 The main purposes for which we use your personal information are:

a. To provide our services to you
To handle your reservations and bookings and to fulfill your travel arrangements and purchases, we need to process most of the information described above. For example, we need your name, passport number and other identifying information to issue your ticket. To confirm your booking and to inform you about changes in your flight status, we need your contact details. And, to ensure that you receive the required care, we require your specified medical needs.

b. To facilitate our loyalty programs
To let you or your company benefit from the discounts and rewards under our loyalty programs, we use your membership information, your booking information and your purchases.

c. To provide our online services and mobile apps to you
• For example, we use your name and flight details when you check-in for your flight with our app.
• Some of our online services and apps use your location, for example to show you the nearest location of your interest.
• To ease your use of our online services or apps, we may analyse the data we collect when you use our digital media and combine it with information collected via cookies and similar technologies (please see above). For example, to understand which digital channel (e-mail, social media) or device (desktop, tablet or mobile) you prefer, so we can restrict our communication to that channel or device.

d. For statistical research
• **General.** We use automatic tools to perform statistical research into general trends regarding the use of our services, loyalty programs, websites, apps and social media and the behavior and preferences of our customers and users.
• **Categories of data.** To perform our research, we may use the categories of personal data described above, including your booking data (such as date of departure, date of arrival, origin, destination, cabin class, number and age of passengers), purchased ancillaries (seats, upgrades), your Flying Blue profile (XP, Miles, tier level) and personal details (gender, postal code). We combine this data with the data we collect with cookies and similar technologies when you visit our websites or use our apps. And we merge it with (aggregated) data collected by third party providers using analytical or marketing cookies or similar technologies. For more information on cookies and similar technologies, please check the cookie policy on our website. We only use aggregated data for our analysis and do not use your name or e-mail address. Without your consent, we will not use special categories of data for this statistical research.
• **Examples.** We use your booking data and the ancillaries you purchase (upgrades, extra luggage) to improve our services and provide more relevant offers. For example, if our research shows that long distance travellers are more inclined to purchase extra legroom, we may include this more prominently in our offers for such flights. We also use customer surveys to measure customer satisfaction and to understand what is important for our customers so we can improve our service. And we use cookies and similar technologies to evaluate how our website visitors navigate our website so we can make it more intuitive.
• **Legal basis.** We process your personal data for our legitimate interests to develop better services and offers for our customers, to improve our loyalty programs, to provide more responsive customer support and to improve the design and content of our websites and mobile apps.
• **Right to object.** You have the right to object, on grounds relating to your particular situation, at any time to processing of your personal data for statistical research (please see below "Your rights").

Source:
https://www.klm.com/travel/gb_en/customer_support/privacy_policy/privacy_policy.htm

7. Data processing agreements

Organisations have to amend numerous data processing arrangements and for this particular piece of compliance they need to be in agreement with another party

Uniform non-customised data protection addenda

Risks:
- Mismatch with existing clauses in the main agreement (liability, audit, subcontracting, contract change…)
- Higher risk that the processing details are not complete

Insufficient detailing on the processing, instructions and/or obligations

Risks:
- Risk of requalification
- Risk of non-compliance core provisions GDPR
- No clear view on which party bears extra costs (assistance, data subject requests…)

Counterparty's implicit consent

Risks:
- Non-enforceability
- Completing processing details needs a discussion
- Subcontracting: (general/specific) authorisation
- Risk of requalification

→ For more important contracts a more customised approach may be necessary

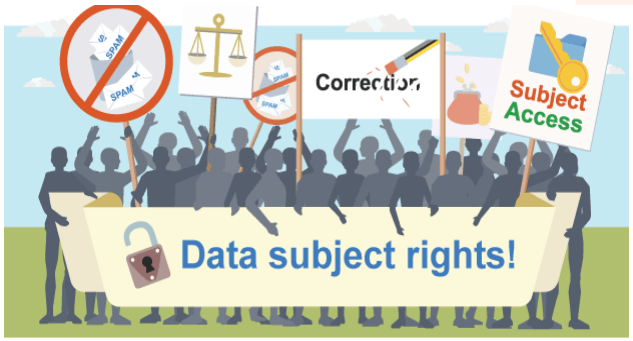
8. Prepare well the handling of data subjects requests

Pre-established procedure

- **First single point of contact**
- **Clear predefined policy** of the organisation on what rights can be exercised in what situation and which data are concerned
- **Management of technical aspects** (how to organise this technically?)

After receipt of request

- Acknowledgement of receipt
- Verification identity data subject
- Verification whether request is founded
- Handle according to predefined policy



Reply

- Respond within one month after receipt of the request (extension permissible on certain conditions)

9. Certification is useful in some circumstances … but not in all

Several companies ask their business partners to provide a certification (often not having one themselves) BUT

No conclusive proof for compliance

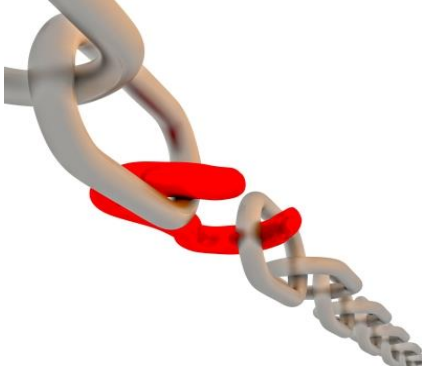
Certification market is not mature

No accredited certification organisation in Luxembourg yet

No reduced responsibility of the controller or the processor (Art. 42 (4) GDPR)

Certification is not just the end, it requests a continuous effort

BUT : CNPD 1st working draft GDPR-CARPA certification mechanism/criteria (1/10/2018)



10. Prepare for data breaches

- Clear **predefined policy** with the course of action to be taken internally
- Draft a risk **charter** setting forth certain categories of threats requiring a particular course of action, in particular a criminal complaint or a breach notification, including criteria under the different applicable legislations as well:

- GDPR
- NIS Directive (and Lux law)
- Sector regulation (telecom, finance)

- Ready made **templates** of notifications and communications to be done in case of a breach

Many GDPR compliance exercises have been done in a rush mode or are not finished…

… so we all know not everything is perfect…

… and this can be dealt with in a GDPR review 2.0!

Questions? At your disposal!

Vincent Wellens
Partner, IP, Technology Law &
Data Protection
T. + 352 26 12 29 34
E. Vincent.Wellens@nautadutilh.com

Carmen Schellekens
Senior Associate, IP, Technology Law &
Data Protection
T. +352 26 12 29 74 06
E. Carmen.Schellekens@nautadutilh.com

Barbara Giroud
Associate, IP, Technology Law &
Data Protection
T. +352 26 12 29 74 27
E. Barbara.Giroud@nautadutilh.com

Faustine Cachera
Associate, IP, Technology Law &
Data Protection
T. + 352 26 12 29 74 12
E. Faustine.Cachera@nautadutilh.com

Emmanuel Thiomé
Associate, IP, Technology Law &
Data Protection
T. + 352 26 12 29 74 15
E. Emmanuel.Thiome@nautadutilh.com

Sigrid Heirbrant
Associate, IP, Technology Law &
Data Protection
T. +352 26 12 29 74 50
E. Sigrid.Heirbrant@nautadutilh.com

Antoine Laniez
Counsel, Litigation and Arbitration
T. +352 26 12 29 17
E. Antoine.Laniez@nautadutilh.com

A brief presentation of our firm

Firm profile

Number of partners, associates and other legal staff.

- An international law firm practising Dutch, Belgian, Luxembourg and Dutch Caribbean law, founded in 1724.
- One of the largest law firms in the Benelux region:
  - 388 lawyers including 72 partners, including 14 female partners.
  - 10 of our lawyers are also university professors.
- Spread across 6 offices and 5 country desks: Offices in Amsterdam, Brussels, London, Luxembourg, New York and Rotterdam.
- Our country desks focus on: Germany, France, India, China and Japan. We also monitor growth markets such as Brazil, Mexico, Indonesia, South Korea and Turkey.
- An independent firm with non-exclusive relations with the top law firms in more than 80 countries.

Office locations