HERBERT SMITH FREEHILLS

Speaker Series 2020 on the GDPR

Dubai

January 22nd 2020

Alexandra Neri – Partner (Disputes – IP/TMT)

The GDPR in figures

Latest GDPR figures on its first anniversary

- **144,376 queries** and complaints from all data protection authorities in Europe since May 2018
- **89,271 data breach** notifications from all data protection authorities in Europe since May 2018
- **Telemarketing**, **promotional e-mails** and **video surveillance** are the types of activities for which most complaints have been made so far

GDPR extra-territoriality principles

Does the GDPR apply outside of the EEA?

The GDPR is binding on companies outside the EU if they process personal data and to the extent that they:

have an "**establishment**" in the EU

OR

offer goods or services to people in the EU or **monitor their behaviour**

e.g. an office, branch, representative or agent

e.g. via a website offering delivery to the EU

Extra-Territoriality: Example

SCENARIO

Company A is located in Dubai

It does not advertise or market its goods directly in to the EU but its website is available in English and customers in the UK can view prices in GBP and order products to be delivered to the UK

The GDPR applies to processing of the personal data of EU data subjects by Company A if that processing is related to the offering of goods or services to EU data subjects

The absence of direct marketing is not relevant if, as a matter of fact, Company A is providing goods and services to EU data subjects

CONCLUSION

The GDPR would apply to the Dubai company's processing of personal data relating to its EU customers

Territorial scope of the GDPR as clarified in the EDPB Guidelines

Establishment criterion: Article 3(1)

- Broad interpretation of "*establishment in the EU*":
  - If processing by a non-EU entity is **inextricably linked to the activities of an EU establishment**, the GDPR applies even if the local establishment has no role in the data processing.
  - But there is no establishment in the EU simply because a non-EU entity's website is accessible from the EU or because the entity uses a data processor established in the EU or has appointed a representative in the EU.

*Example: a single employee in the EU may constitute an "establishment" within the meaning of the GDPR, but the presence of an employee in the EU as such does not trigger the application of the GDPR. The GDPR only applies to data processing activities that are **related to the activities of the EU-based employee** and not to data processing activities that relate to the activities of a controller outside the EU.*

Territorial scope of the GDPR as clarified in the EDPB Guidelines

Offering goods and services to people in the EU or monitoring their behaviour: Article 3(2)

- The GDPR applies to processing concerning people **located** in the EU, regardless of their citizenship or residence (e.g. applies to people transient in the EU such as tourists)
- The offering of services also includes the offering of "***information society services***"
- Monitoring is not limited to tracking behaviour on the internet, but includes ***tracking through other types of networks*** or technology (e.g. wearable and smart devices)

Case: A marketing company established in Dubai provides advice on retail layout to a shopping centre in France, based on analysis of customer movement throughout the centre collected through Wi-Fi tracking.
➔ *The GDPR would apply to the Dubai company's processing of personal data relating to French customers.*

Territorial scope of the GDPR as clarified in the EDPB Guidelines

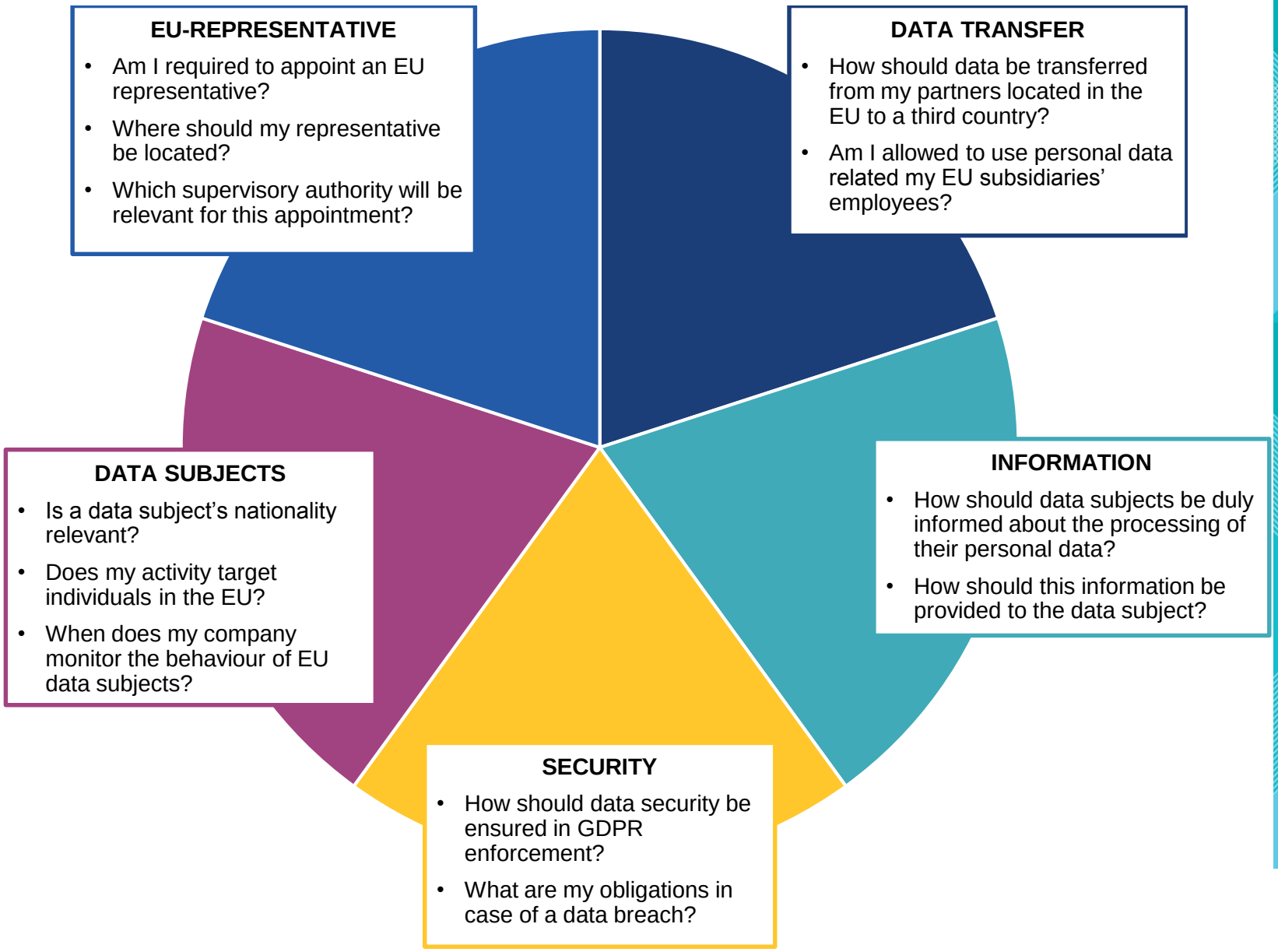
Applying this criterion to data controllers and processors

- A processor not subject to the GDPR will **become indirectly subject to some obligations imposed on controllers subject to the GDPR** by virtue of mandatory contractual arrangements under Article 28 of the GDPR.
- The processing activities of a data controller established outside the EU (and not subject to the GDPR as per Article 3(2)) would not fall under the territorial scope of the GDPR merely because the data are processed on controller's behalf by a processor established in the EU. **Nevertheless, the processor is subject to relevant GDPR provisions directly applicable to data processors**.

"In line with the positions taken previously by the Article 29 Working Party, ***the EDPB takes the view that the Union territory cannot be used as a "data haven"****, for instance when a processing activity entails inadmissible ethical issues, and that certain legal obligations beyond the application of EU data protection law, in particular European and national rules with regard to public order, will* ***in any case have to be respected by any data processor established in the Union, regardless of the location of the data controller****." (EDPB)*

The biggest GDPR compliance issues for non-EU companies

MOST COMMON QUESTIONS ABOUT GDPR COMPLIANCE



EU-REPRESENTATIVE

- Am I required to appoint an EU representative?
- Where should my representative be located?
- Which supervisory authority will be relevant for this appointment?

DATA TRANSFER

- How should data be transferred from my partners located in the EU to a third country?
- Am I allowed to use personal data related my EU subsidiaries' employees?

INFORMATION

- How should data subjects be duly informed about the processing of their personal data?
- How should this information be provided to the data subject?

SECURITY

- How should data security be ensured in GDPR enforcement?
- What are my obligations in case of a data breach?

DATA SUBJECTS

- Is a data subject's nationality relevant?
- Does my activity target individuals in the EU?
- When does my company monitor the behaviour of EU data subjects?

GDPR compliance issue example: CNIL v. GOOGLE

On January 21, 2019, the French Data Protection Authority (CNIL) fined Google LLC 50 million euros

Google LLC has its headquarters in California. The Irish subsidiary Google Ireland Limited was not considered as a “main establishment” by the CNIL because:

- Google Ireland did not have any decision-making powers regarding the processing governed by the privacy policy presented to the user on creating an account, and when configuring their mobile phone under Android;
- Google Ireland was not referred to in the company’s “Privacy Policy” dated 25 May 2018 as being the entity where main decisions are taken as regards the purposes and the means of processing governed by the privacy policy presented to the user on creating an account, and when configuring their mobile phone under Android;
- Google Ireland has not appointed a Data Protection Officer in charge of the personal data processing that it may carry out within the EU;
- The Android operating system is only developed by Google LLC.

On January 21, 2019, the French Data Protection Authority (CNIL) fined Google LLC 50 million euros

Two GDPR grounds were at stake:

- Transparency and information obligation
  - The information that should be communicated to individuals was spread across several documents, thus infringing Article 13 because of lack of transparency;
  - The information given to the user was too vague, thus infringing Article 12.
- Obligation to have a legal basis for ads personalization processing
  - The users' consent was not sufficiently informed, thus infringing Article 4;
  - For example, the information provided in the "Personalized advertising" section included: *"Google can show you ads based on your activity on Google Services (ex: Search, YouTube, an on websites and apps that partner with Google)"*. However, it was impossible to find the Google services, sites and apps to which the company referred. Therefore, the user was not able to understand the personalized advertising processing and the amount of data collected.

Dealing with legal issues raised by the GDPR

Issues related to transparency 1/2

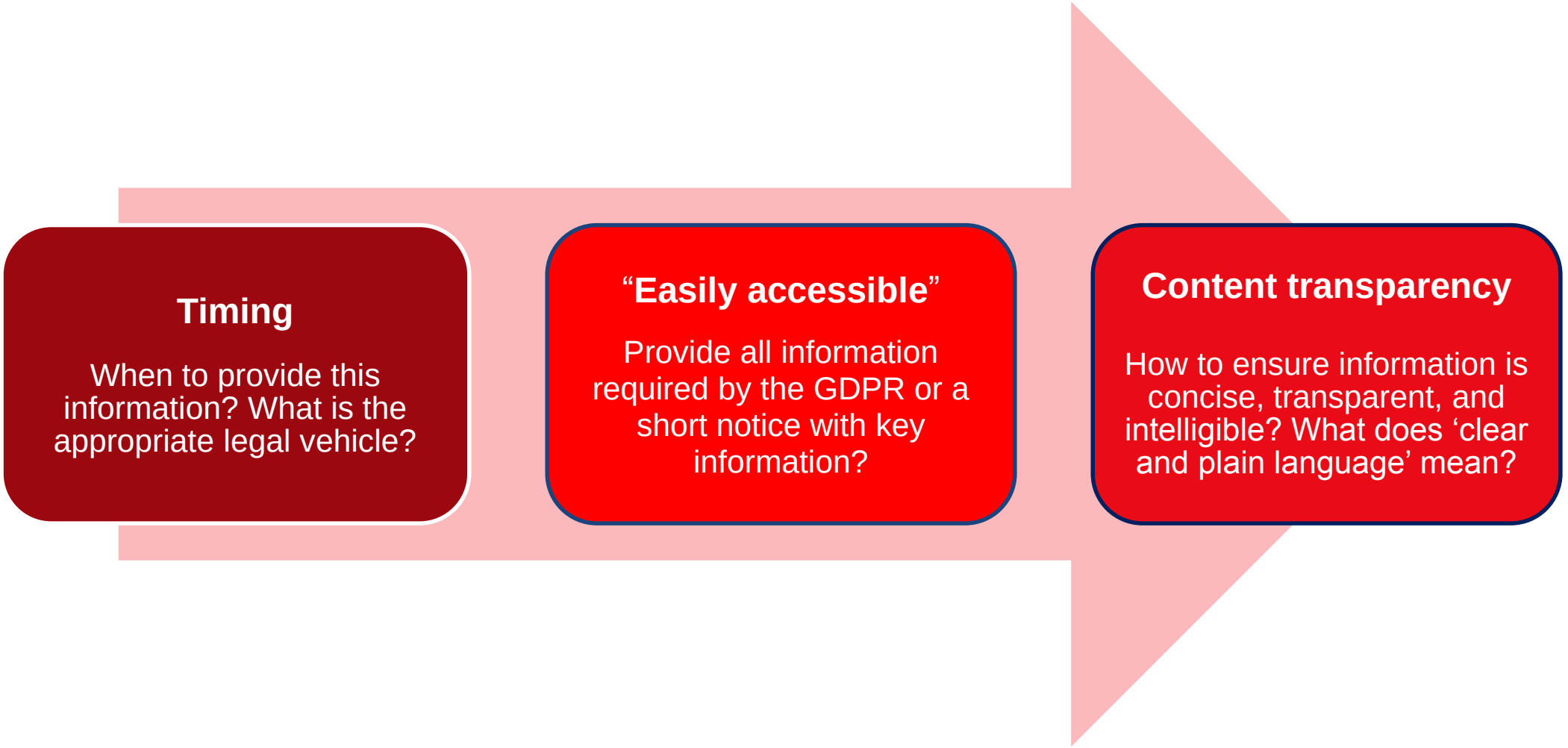
ARTICLE 5 - "*1.(a) Personal data should be processed […] in a **transparent manner** in relation to the data subject" (cf. articles 12, 13 and 14 of the GDPR regarding information to be provided)*

Data controllers must include more information for data subjects in their fair processing notices

- Retention periods for each type of data (or criteria used to determine)
- Clear and straightforward guidance for data subjects about their rights, including process for withdrawing consent
- Clear and transparent information about parties to whom personal data will be disclosed
- Details of how personal data will be processed and legal basis for each processing activity

Issues related to transparency 2/2

How should you provide transparency information?



Issues related to personal data transfers

ARTICLE 44 "*Any transfer of personal data* which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this [Chapter V] are complied with by the controller and processor […]."

How should you transfer personal data to third countries?

EXCEPTION

Is the data transfer covered by one of the 'exceptions' set out in Article 49 of the GDPR?

(*necessary to perform a contract, consent of the data subject, necessary to establish a legal claim, make a legal claim or defend a legal claim, etc…)*

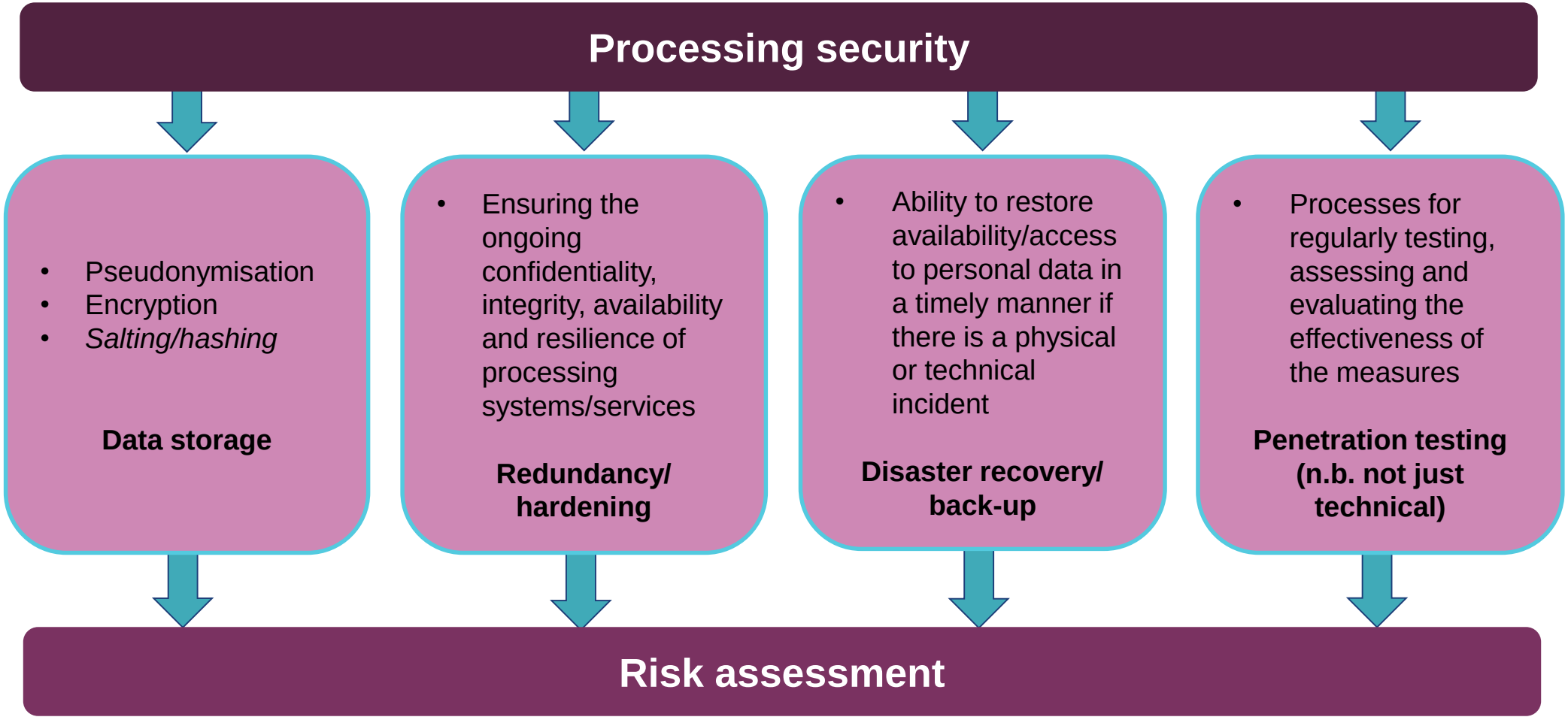
APPROPRIATE SAFEGUARDS

* Draft a data transfer agreement containing the **standard data protection clauses** adopted by the Commission, to be signed by the data exporter and the data importer.

* **Binding corporate rules** could also be signed to allow multinational corporations, international organizations, and groups of companies to make intra-organizational transfers of personal data across borders.

Issues related to processing security 1/2

ARTICLE 32 - "*1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall* ***implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*** *[…]*"



Issues related to processing security 2/2

How should clauses be tailored to ensure security?

- Ensure that the division of labour for cyber security is clear, e.g. in a telecoms infrastructure project, the contractual framework will usually have cyber security schedules that define exactly what each contractor is responsible for and the customer dependencies

- Take care at the interfaces between systems that individually would otherwise be secure – try to avoid security “gaps” caused by other suppliers – or ensure that these do not become your problem by defining the borders

- Consider whether the relevant definitions are appropriate to the systems and services to be provided. If you have a standard suite of definitions, these should form the basis of negotiations

Issues related to data breaches 1/2

ARTICLE 33 "*In the case of a personal data breach, the controller shall* ***without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach*** *to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. […]."*

Informing affected persons

Notification of regulatory authorities

Legal Containment (e.g. reputation)

Informing people affected by an incident

- When? (after occurrence or after resolution)?
- How? (appropriate channels of communication)
- Who? (public announcement/tailored email etc.)

Obligations to report cyber security incidents: new developments in Europe

- Already applies to communications service providers (Regulation 611/2013)
- Cybersecurity (NISD) Directive
- General Data Protection Regulation: applies to all data controllers and foreign companies doing business in the EU

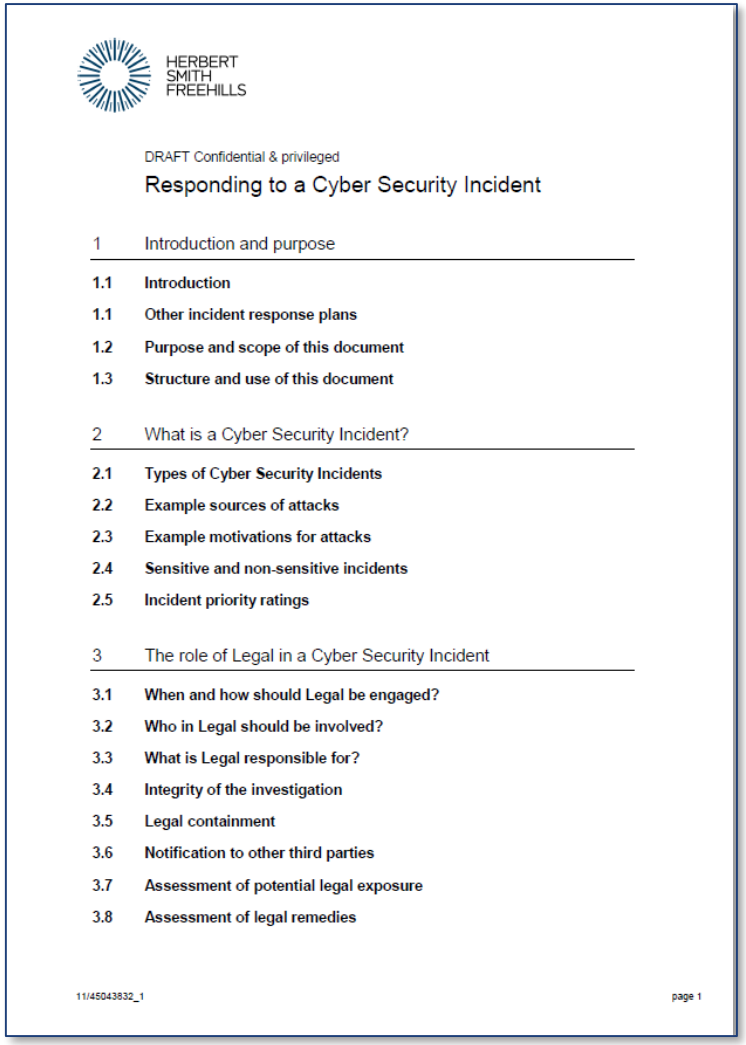
Developing a litigation strategy if the company's reputation is affected

- Ex parte petitions against tech intermediaries to identify perpetrators and obtain injunctions
- Action against hosting companies/domain name registries to get leaked data/information taken down
- Media management (e.g. injunction applications)

Issues related to data breaches 2/2

How should legal incident response planning be organised?

- Legal containment
- Multi-national notification requirements
- Contractual notification requirements
- Insurance coverage and requirements
- Document and evidence preservation



HERBERT SMITH FREEHILLS

DRAFT Confidential & privileged

Responding to a Cyber Security Incident

1 Introduction and purpose

1.1 Introduction
1.1 Other incident response plans
1.2 Purpose and scope of this document
1.3 Structure and use of this document

2 What is a Cyber Security Incident?

2.1 Types of Cyber Security Incidents
2.2 Example sources of attacks
2.3 Example motivations for attacks
2.4 Sensitive and non-sensitive incidents
2.5 Incident priority ratings

3 The role of Legal in a Cyber Security Incident

3.1 When and how should Legal be engaged?
3.2 Who in Legal should be involved?
3.3 What is Legal responsible for?
3.4 Integrity of the investigation
3.5 Legal containment
3.6 Notification to other third parties
3.7 Assessment of potential legal exposure
3.8 Assessment of legal remedies

11/45043832_1 page 1

- Guidelines for internal witness interviews
- Guidelines for post-incident communications
- Guidelines for email communications and distribution lists
- Template take-down notices, undertakings, notifications to regulators, PR comms, etc
- Liaison with law enforcement

THANK YOU