ADSTO
Avocats à la Cour

IFCLA

GDPR liability related to IoT devices imported to the EU

September 30, 2021

ADSTO - Claire BERNIER - Partner

ADSTO
Avocats à la Cour

IOT: WHAT DOES IT MEAN?

internet connected devices able to collect, store, process and spread data or able to fulfil specific actions according to the received data

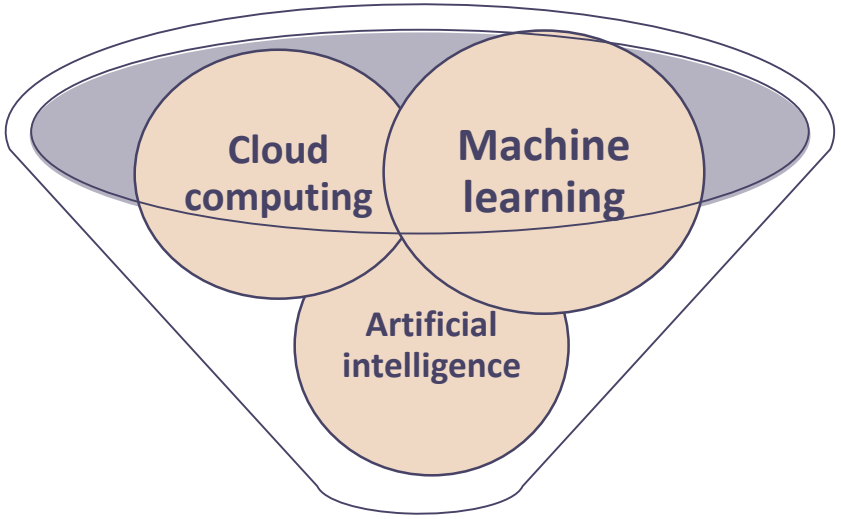
Encouraging technology?

2,5 exabytes are produced per day = 167,000 time more than US Congress library's data*

**OCDE 2015, Data-driven innovation : Big Data for Growth and Well-being, OCDE Publishing, Paris, p. 20*

22 billion IoT devices connected today, experts foresee this number to be more than 75 billion by 2025

how such a technology is built?



INTERNET OF THINGS

ADSTO
Avocats à la Cour

IOT: WHOM FOR? WHAT FOR?

PERSONAL DATA ▪▪▪▪▪▪▪▪▶ VALUABLE RESOURCES

ECONOMY

- Global market estimated at $54,3 billions in 2018
- World Economic Forum estimates that the personal data market could generate $500 billion by 2024

HUMANITY

- E.g. Better self-knowledge, improve their physical skills, etc.
- E.g. Tremendous opportunity for science to learn some global health issues and seek resolution

JUSTICE

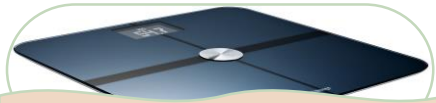
- E.g. Helpful with the burden of proof
- E.g. Data used as evidence

ADSTO
Avocats à la Cour

WHAT BENEFIT FOR IOT USERS?

seek for new medical supports with dematerialization process

Connected watch



Connected scales

Connected toothbrush

seek for more security, driving assistance, various helper system for mobility

Connected camera

Connected windscreen with augmented reality

Bluetooth tracker

seek for improvement of natural skills, for perfect movements

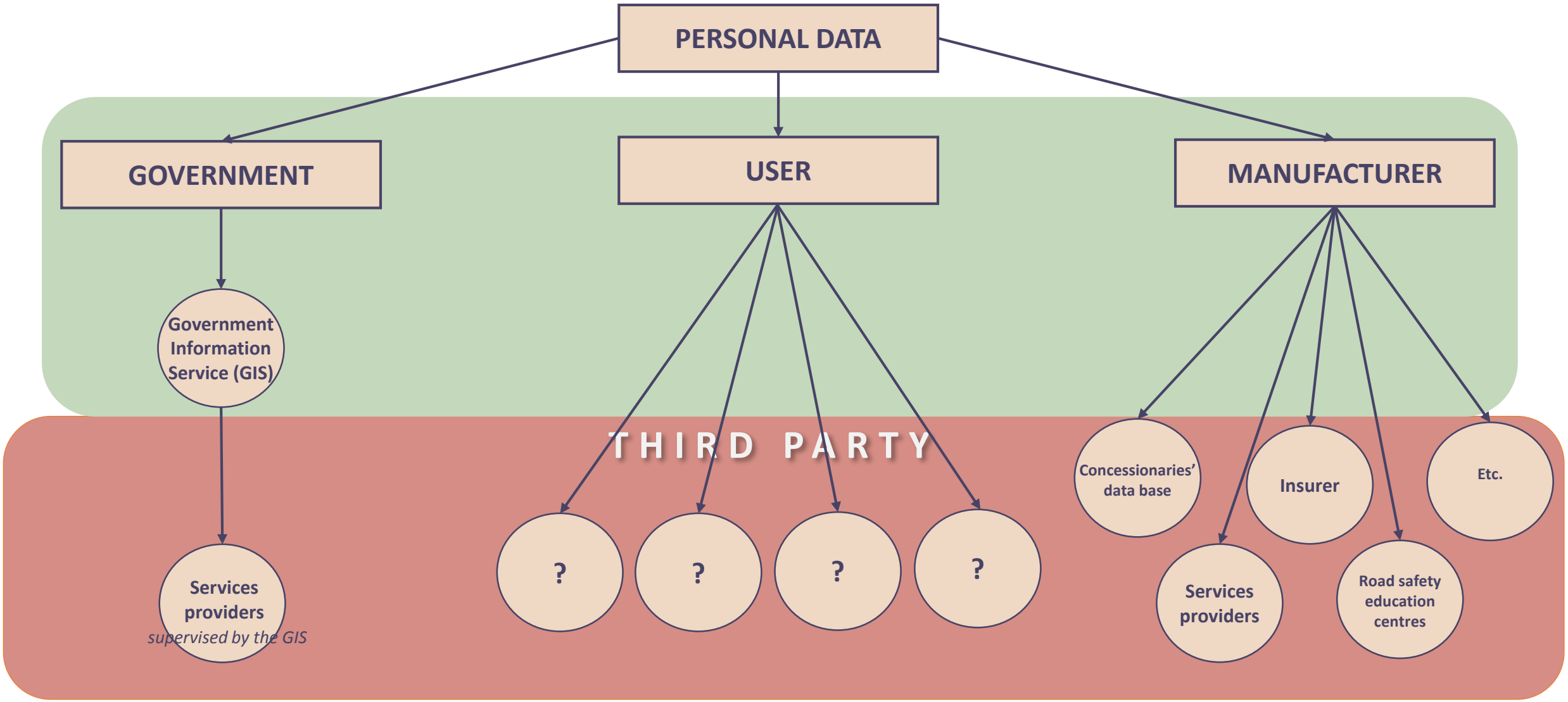
Connected jacket

Connected dancer point shoes

IFCLA

ADSTO
Avocats à la Cour

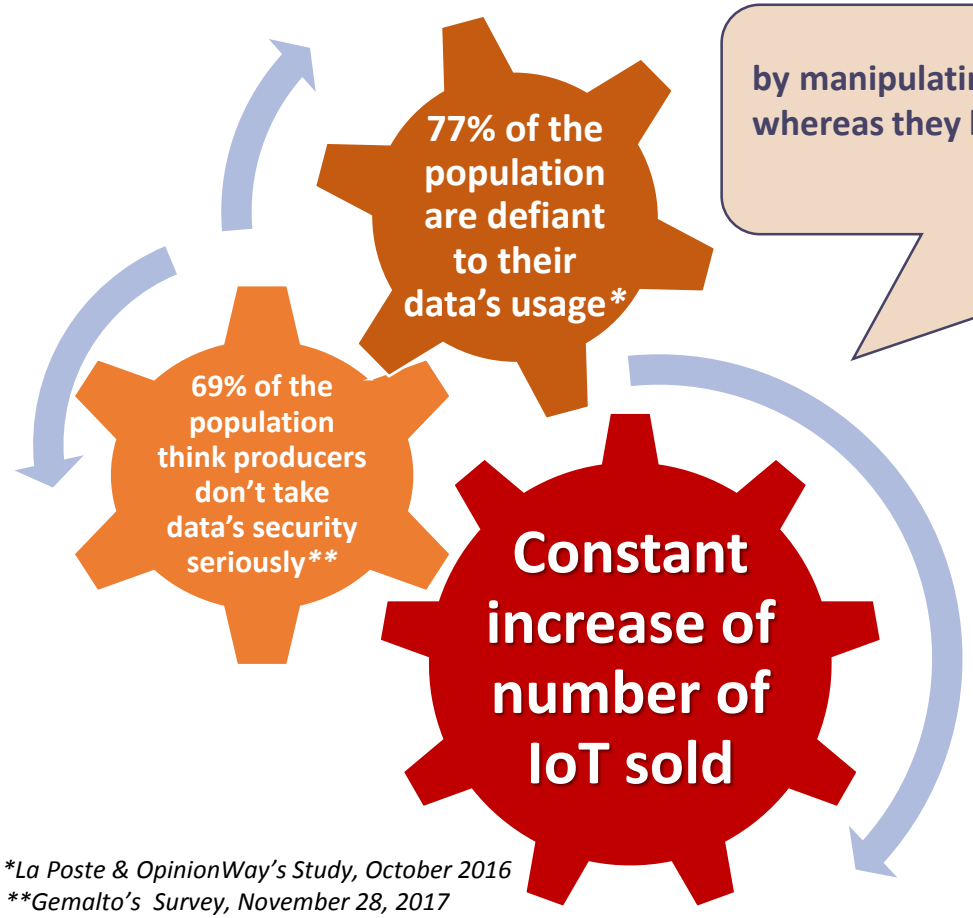
IOT & DATA SPREADING



ADSTO
Avocats à la Cour

IOT & PRIVACY PARADOX

judging by the increase of IoT devices purchased.



by manipulating their device, users "feel" their data becoming more real, whereas they look invisible on the web.

e.g. covid-19 government's apps

CYBERATTACKS

4th & 5th in top 10 risks

*La Poste & OpinionWay's Study, October 2016
**Gemalto's Survey, November 28, 2017

ADSTO
Avocats à la Cour

DATA COLLECTED BY IOT DEVICES = PERSONAL DATA ACCORDING TO GDPR

- ***Art 4 paragraph 1 GDPR*** **defines** **personal data** **as** ***"any information relating to an identified or identifiable natural person"***
- ***Art 4 paragraph 15 GDPR*** **defines** **data concerning health** **as** ***"personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"***

HEALTH AND FASHION/CLOTHES		VEHICLE
CNIL Health Working Group 18 Nov 2019	***Art 4 par.13 & 14 GDPR***	***Conformity Pack CNIL 17 Oct 2017***
collected data by health following apps or connected watches **are** data concerning health by purpose and, must be regarded as **sensitive data** depending on their level.	**genetic data**: personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health (…) **biometric data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person (…)	• **IN-IN**: data strictly related to the user, such as identity, date of birth, etc. => no handover to the supplier. • **IN-OUT**: data strictly related to users and vehicles' occupiers : biometric and kilometre data, on board data, such as air conditioning, music, etc. => handover to the supplier. • **IN-OUT-IN**: data related to the vehicle itself (GPs tracking, number plate, wear, etc.) => external handover. • ***Avril 14,2021's ruling***: notification requirement for manufacturer about the data process.
PERSONAL DATA ***(sensitive data)***	**PERSONAL DATA** ***(sensitive data)***	**PERSONAL DATA**

ADSTO
Avocats à la Cour

IOT & GDPR SCOPE

Cf. art. 2 & 3 GDPR on material and territorial scope

	MANUFACTURER		DATA CONTROLLER		USER		GDPR
	IN EU	*OUT EU*	*IN EU*	*OUT EU*	*IN EU*	*OUT EU*	
SITUATION 1	X		X		X		✓
SITUATION 2	X		X			X	✓
SITUATION 3	X			X	X		✓
SITUATION 4	X			X		X	X
SITUATION 5		X	X		X		✓
SITUATION 6		X	X			X	✓
SITUATION 7		X		X	X		✓
SITUATION 8		X		X		X	X

ADSTO
Avocats à la Cour

IOT & GDPR BREACH

- **User suffering from a material or moral damage because of a breach of their personal data can ask for reparation.**
- ***Art. 24 GDPR*: *liability of the data controller.***
- ***Art. 26 GDPR*:** *where two or more data controllers jointly determine the purposes and means of processing, they shall be joint controllers* **=> *joint-liability.***
- ***Art. 27 GDPR: where Article 3(2) applies, the data controller or the processor shall designate in writing a representative in the Union.***

  (nb: art 3(2) GDPR: This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
  - *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
  - *the monitoring of their behaviour as far as their behaviour takes place within the Union.)*

- **Art 84 GDPR: "*Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83* [nb: General conditions for imposing administrative fines]*, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive*."**

- **The amount of financial penalties may be up to €20 million or in the case of a company up to 4 % of the global annual turnover. E.g. of recent fines and penalties which data protection authorities within the EU:**

DATE	FINE (€)	DATA CONTROLLER	GDPR BREACH
2021-09-24	900,000	Vattenfall Europe Sales GmbH	Transparency and modalities, Information to be provided where personal data are collected from the data subject
2021-09-14	40,000	Vodafone España, S.A.U.	Lawfulness of processing
2021-09-02	225,000,000	WhatsApp Ireland Ltd.	principles relating to processing of personal data, information to be provided where personal data are collected from the data subject, information to be provided where personal data have not been obtained from the data subject

RESPONSIBLE = MANUFACTURER, DATA CONTROLLER POTENTIALLY SUPPLIERS AND INTERMEDIARY.

financial penalty according to GDPR and to national laws + criminal penalty according to national laws

➢ **CONNECTED DEVICES = MEDICAL DEVICE ?**

World Health Organization	**monitoring devices**	✓
French High Health Authority	**connected devices**	✓

AID FOR DOCTOR?

- Medicinal freedom on diagnosis ? if there is a fault, then he is responsible.
- Defective device ? manufacturer's responsible because of defective devices's liability.

ADSTO
Avocats à la Cour

OTHER LIABILITIES

NATIONAL LAWS

- CUSTOMER LAW
- DEFECTIVE DEVICES
- CUSTODY OF THE THING
- CRIMINAL LAW

CORPORATE SOCIAL LIABILITY

- **The CNIL** *(French National Data Authority)* **may impose all the administrative sanctions provided for by the GDPR but may also impose criminal sanctions in the event of non-compliance with the GDPR.**
  - **E.g. Art.226-21 Criminal Code:** *misappropriation of the purpose of personal data = 5 years in prison and a €300,000 fine.*
  - **E.g. Art R625-10 Criminal Code:** *non-compliance with the rights of individuals = fine of €1,500 for each breach.*
  - **E.g. Art R625-12 Criminal Code:** *lack of information from data subject = fine of €1,500 for each offence.*

TODAY

FUTURE ?

DIGITAL LIABILITY?

IoT liability = give IoT's their own liability, which implies their own legal personality

Robot liability = give robots their own liability, which implies their own legal personality

Interest of the European Commission and Parliament

crucial issue that required an EU-wide response through a specific legislative package combined with guidelines and codes of conduct.

what liability regimes? "strict liability principle" vs "risk-based liability principle

DELVAUX REPORT, 2017

eventual creation of a legal personality for robots, considered as electronic persons making their own actions.

ADSTO
Avocats à la Cour

HEALTH DATA HUB CASE: *FRENCH ADMINISTRATIVE SUPREME COURT (CONSEIL D'ETAT – CE), OCTOBER 13, 2020, N°444937*

FACTS

- **Health Data Hub is a collect tool used to centralize health data for the purpose of analysis and research => introduced since December 2, 2019 under the watch of The National Institude of Health Data.**
- **Data are stored on a Microsoft's Cloud in Ireland.**
- **N.B. Microsoft is subject to the american law which *"compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil."*** *(Clarifying lawful overseas use of data act ou cloud act (H.R. 4943), 6 févr. 2018)*

PROCEDURE AND DEFENCE

- **The French Health Department requests the invalidation of the contract which appoints Microsoft Ireland Ltd as the web host in behalf of *art.L3131-1 of Public health code: "In the event of a serious health threat requiring emergency measures, the Minister prescribes […] any measure proportionate […] in order to prevent and limit the consequences of possible threats to the health of the population"* as a breach of personal freedom.**
- **CNIL statement of case: Cloud Act doesn't assure guarantees of a suitable protection. To ground its defence, CNIL adds that such a partnership breaks the *Schrems II's* decision rendered by the CJUE** *(July 16,2020, C-311/18)* **and the GDPR's art. 48.**

CONSEIL D'ETAT DECISION

- **The CE held that by the additional provision dated September 2, 2020 mentioned at the end of Microsoft agreement, Microsoft commits not to process data stored out of Europe. In October 9, 2020, French Health Department took a decree prohibiting all transfers of health data outside the European Union.**
- **Thus, The French Administrative Supreme Court confirmed that temporarily Microsoft Ireland Ltd can be the web host, judging that it was not necessary to cease the platform's activity.**
- **Nevertheless, CE imposes a closer inspection by CNIL to reinforce data protection and avoid breaches.**

As a reminder, CNIL initially did not approve Microsoft's warranty of data protection.

ADSTO
Avocats à la Cour

IOT & IMPACT ASSESSMENT

Art. 35 **about the impact assessment:** ***"where a type of processing in particular using new technologies[…] is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."***

CNIL release a non-limited table listing the data process submitted to an impact assessment. *E.g.*:

- ❑ Health data processing carried out by health or medical establishments for the treatment of persons.
- ❑ Treatments involving genetic data of so-called vulnerable persons
- ❑ Processing intended to constantly monitor the activity of the employees concerned

But also a non-limited table listing the data process not submitted to an impact assessment. *E.g.*:

- ❑ Treatment of supplier relationship management.
- ❑ Processing of health data necessary for the management of a patient by a health professional working in an individual capacity within a medical office, pharmacy or medical biology laboratory.

Does my IoT data process is on the CNIL case list where an impact assessment is mandatory ?

YES

NO

How many criteria my process fills ?

1. Scoring, profiling
2. Automatic decision with legal effect or similar
3. Systematic supervision
4. Sensitive data or highly personal *(health,etc.)*
5. Large-scale collection
6. Cross-referencing data
7. Vulnerable people *(elderly, children,etc.)*
8. Innovative use
9. Exclusion from a right/contract

AT LEAST TWO

OR

ONLY ONE BUT MY PROCESS SEEMS HIGHLY RISKY

NONE

IMPACT ASSESSMENT REQUIRED

IMPACT ASSESSMENT NOT REQUIRED

(but should respect data protection principles and the rights of the affected people)

IFCLA

ADSTO
Avocats à la Cour

IOT & GDPR: SOME PRACTICAL GUIDELINES

BEFORE THE PROCESS

- Raise user's awareness on their collected personal data, rights and good behavior.
- Authenticate the said user and limit access to only data that a user needs.
- Provide for an impact assessment if required.
- Provide a breach follow-up with a development notebook (in order to identify each breach and seek for a remedy).
- Secure applications and equipments (servers, websites) a all the movable informatics.

AFTER THE PROCESS

- Erase data after the authorised retention period.
- Frame the upkeep and the data destruction.
- Make sure to comply with GDPR obligations regarding data's safety with the subcontractors and IT developments.

ADSTO
Avocats à la Cour

IFCLA

THANK YOU

Claire BERNIER ADSTO +33(0)6 73 80 26 37 24 boulevard de Douaumont 75017 clairebernier@adsto.legal