As new digital technologies such as AI, the Internet of Things, big data, advanced robotics emerge bringing forth new products, platforms and services (smart environments, autonomous cars, robots and drones, face recognition cameras, etc.), the allocation of liability when things go wrong can prove complex. In the case of collaborative information management systems, there are several cross-cutting legal instruments that would potentially regulate different liability aspects, such as the European Product Liability Directive, the Electronic Commerce Directive, the Radio Equipment Directive and the General Data Protection Regulation (GDPR). The interaction of these distinctive sets of rules is a complex exercise and very much depends on the chosen exploitation model of the system. In this respect, when setting up a collaborative information management system, it is recommended to distinguish between potential liability of partners and collaborators (i.e. the entity providing and hosting the collaborative information management system's infrastructure (host), the entity that developed the system's software and/or hardware, and the first responder agencies using the system).

Guiding Questions

Who develops and who hosts the collaborative information management system?

Are there Memoranda of Understanding?

Is there a central entity provisioning the system's infrastructure and could it benefit from certain liability exemptions?

Have you identified which actors should comply with the security requirements laid down in the GDPR?

Further Information

According to the EU Commission Staff Working Document (SWD (2018) 137), a working definition of 'liability' is the responsibility of one party for harm or damage caused to another party, which may be a cause for compensation, financially or otherwise, by the former to the latter.

In regards to the development of a collaborative information management system, the allocation of liability can be a complex exercise which very much depends on the chosen exploitation model of the system and as such will be subject to several cross-cutting legal instruments that regulate different liability aspects. Some of there are:

European Product Liability Directive: The first corpus of rules that should be taken into account concerns the European Product Liability Directive since the software and hardware created for and used by a collaborative information management system are considered to be products that fall within its scope. This directive, that has been transposed into national laws, imposes a strict liability regime on producers. They will be held liable for damage caused by the malfunctioning of the product without the proof of a fault.

Electronic Commerce Directive: The Electronic Commerce Directive might be of relevance when assessing the liability of the central actor who would be providing the system's architecture to interested first responder agencies who would like to interconnect. If some kind of illegal content would be communicated between the different parties, the host of the general infrastructure could benefit from certain liability exemptions laid down in this instrument.

General Data Protection Regulation (GDPR): Data protection legislation and failure to comply with the security requirements of the General Data Protection Regulation (GDPR), could also trigger liability. In the context of data protection compliance all of the participants should ensure the secure processing of personal information at every single stage of the processing chain. First of all, this implies that the servers on which each single national agency (the connected entity) stores this information for their own purposes are safe. Secondly, this requires that the transmission via the collaborative information management system takes place in a secure way. This can be either a shared responsibility or a responsibility borne by a single organisation that hosts the system's infrastructure (host). Therefore, the system itself should be designed to accommodate different kinds of security policies and allow for the implementation of a number of precautionary measures, such as the encryption of the information during the communication process.

Furthermore, the addition and use of emerging digital technologies such as IoT, AI, autonomous drones, etc. in a collaborative information management system can raise additional questions in regards to liability. Specifically, the increasing connectedness and complexity, in terms of design and system integration, of such products and services raises the issue of whether effective redress mechanisms for victims and legal certainty for producers can still be possible. Characteristics such as increased autonomy and self-learning, for example, can prove challenging where the damage caused by the autonomous machine cannot be linked to a defect or human wrongdoing. Or, the presence and use of faulty or corrupted data (for example, due to hacking or connectivity problems) can be considered a service malfunction rather than a product one. As such, it would fall outside the European product liability and safety regimes and within national law. Still, where damage is caused by the supply of erroneous data or by a failure to supply data, allocating

liability may become unclear and claims potentially difficult to enforce (EU SWD 2018).

Examples

This table provides an overview of the security requirements (art. 32 GDPR) in order to comply with the GDPR. It also identifies which actor is responsible for the implementation of each requirement. Each actor can be held liable in case of non-compliance with that specific requirement:

Requirement Description	Implementation Example	Responsible Actor
Encryption of personal data	Data sent to the system should be encrypted in order to secure the transmission of personal data.	Shared responsibility
Measures for pseudonymisation of personal data	Replace direct identifiers by a proxy.	Connected entity
Confidentiality	Confidentiality can be guaranteed by introducing virtual communication groups in which only certified trusted parties can participate.	Shared responsibility
Integrity, availability and resilience of processing systems and service	Distributed structure, hosted at the participants' servers, and peer-to-peer message distribution with a synchronisation design. This architecture allows the collaborative information management system to continue working even if the connectivity is partly down, and to resume the full information after re-connection.	Shared responsibility

Testing of technical and organisational measures for ensuring the security	Testing can take place within the context of a disaster exercise.	Shared responsibility
Ensure that any natural person who has access to personal data does not process them except on instructions from the controller.	A collaborative information management system is a communication system. Personal credentials of users have to be checked by the owners of the connected tools.	Connected entity

Resources

Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (Product Liability Directive) [Link]

Council Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [Link]

EU Commission Staff Working Document (2018) Liability for emerging digital technologies [Link]

GDPR Overview of the General Data Protection Regulation (2017). Information Commissioner's Office [Link]

Kuczerawy A. and Ausloos J. (2015) NOC online intermediaries case studies series: European Union and Google Spain. *NOC Report on Internet Intermediaries Liability*, February 2015. [Link]