



STORMSHIELD

OPINION ARTICLE

HOW DO YOU DEFINE SENSITIVE DATA?

Victor Poitevin
Editorial & Digital
Manager, Stormshield

Personal, sensitive, critical and even vital... there are so many words to describe data. This may also lead some companies and organizations to believe that data protection is not an issue that concerns them. But is that really true? Could personal data, as highlighted by the GDPR, be the tree that prevents us from seeing the woods? After all, all companies produce data, but not all of them are aware of its value. Or, indeed, the need to protect such data.

Since coming into force in May 2018 in Europe, the General Data Protection Regulation (GDPR) has contributed to the spread of new expressions: personal data and sensitive data. A few moments with a search engine quickly reveals just how much of a current preoccupation sensitive data is. But what exactly does this mean? Because on closer inspection, the field of sensitive data is rather limited, and under its strict definition, clearly falls short of covering all of the company's data issues. And yet...



WHAT IS SENSITIVE DATA?

The European Commission's list defining sensitive data under the GDPR is clear. These are personal data pertaining to a person; that is, information relating to their racial or ethnic origin, political opinions, religious or philosophical convictions, trade union membership, genetic or biometric data, health data, sex life or sexual orientation.

The processing of such data, including their collection and use, is strictly regulated by law. But is this the only form of data that requires special protection? Spoiler alert: no..


SENSITIVE, CRITICAL, VITAL DATA, ETC.


That's because the many forms of data in an organization go way beyond merely sensitive data. In its best computing practice guide (in French), the French agency ANSSI refers to *"data deemed vital for the organisation and the servers in question."* This is a new way of talking about data. So, what is the difference between sensitive data and vital data? Vital data are considered essential to the entity's ability to function normally: production data, financial data, R&D data (the secret recipe for a drink or the algorithm for a search engine, for example, etc.). Without them, the company ceases to exist, or loses its competitive advantage. These are data that, if revealed, stolen or lost, would have a critical impact on the business or organization suffering its loss. For example, data relating to a current negotiation, a fundraising round or an upcoming takeover bid. But there's more to it than just that. Deny access to a simple order book, and the entire business activities of a small company can be compromised. **The spectrum of data requiring protection is therefore much broader than just sensitive data.** And all such data is a target for cybercriminals. *"Indeed, an increasing number of small organisations are being hit by attacks aimed at denying access to such data"*, the ANSSI emphasises in its guide. As such, they require special care, with regular backups (stored on offline equipment), with test restores also being performed periodically.

"We often think first of strategic data: HR or financial data, R&D or production data... but in fact, there is value in any data produced by the company. If we have taken the time to produce it, it must be because it contributes to the activity of the company. It must therefore be protected too."

Julien Paffumi, Senior Product Manager at Stormshield

Personal data, sensitive data, vital data or even critical data, the data to be protected vary from one organization to another: know-how on chemical processes, R&D, locations of raw materials, internal audits (protection of figures, investments, etc.), correspondence between members of the Executive Committee, buyout/takeover bids, HR data, accounting data, correspondence between journalists and their sources,





production lines, industrial parts diagrams, etc. “At Stormshield, for example, CVs are exchanged via encrypted emails. And shared staff data are stored in secure directories,” explains **Jocelyn Krystlik**, Business Unit Data Security Manager at Stormshield. “Data that are classified as critical affect or comprise the core business of a company: patents, commercial activity, financial data, strategic data, etc. In other words, anything that has a value recognized by its customers. We must therefore think in terms of information and the way in which that information is strategic for the organization,” says Data Specialist **Laurence Houdeville**, co-author of the white paper *The trust cloud: a strategic autonomy issue for France*. This includes refined data, obviously... but more besides.

“More or less all company data is important and useful,” points out **Julien Paffumi**, Senior Product Manager at Stormshield. “We often think first of strategic data – HR or financial data, R&D or production data, and so on – but in fact, there is value in any data produced by the company. If we have taken the time to produce it, it must be because it contributes to the activity of the company. It must therefore be protected too. This is also true of unstructured data”. According to Gartner’s Magic Quadrant for Distributed File Systems and Object Storage, the annual growth rate of unstructured data is of the order of 30 to 60%. And according to a study by Thales, a mere 17% of businesses encrypt at least half of their data in the cloud. These two figures show the key importance of data protection. But how do you go about it?


IDENTIFYING AND CLASSIFYING DATA TO PROTECT IT BETTER


According to Laurence Houdeville, “we only properly protect what we properly know.” **The first issue of data protection, therefore, is to know your information assets.** In practical terms, this means inventorising data processing operations (whether automated or not), processed data (e.g. customer files, contracts) and the media on which they are based – in terms not only of equipment (e.g. servers, laptops, hard disks) and software (e.g. operating systems, business software) but also communication channels (e.g. optical fibre, Wi-Fi, Internet).

“We only properly protect what we properly know.”

Laurence Houdeville, data specialist

“We create an inventory with a map showing the reference data, asking the questions: which data have the most value, and when are they used? So the real interest lies not in the utility data but in the refined, cross-referenced data,” Houdeville explains. Then we work on the critical path: how are these data cross-referenced with other data, what criteria reveal the value of these data?, etc.” Following the audit, **data classification** can be used to sort according to the criticality of the data, and therefore their confidentiality and dissemination. That may be true, but here’s the problem: there is no standard






nomenclature. *"Each organisation has its own classification levels: C1, C2, C3 (1st level confidential, etc.); D1, D2, D3; internal or external... and even colour-coded (amber / red...)"*, Krystlik explains. *"There is no standardisation: everyone does as they see fit, even though the contexts are all more or less the same."* So – as is often the case – it boils down to a question of cyber maturity.

ORGANISATIONAL MATURITY IN RELATION TO DATA

There are different solutions for classifying data: a universal template with fillable fields, a watermark in the file or automatic classification using words or key information (social security number, bank details, etc.). *"Small businesses often provide an email template where users enter the classification themselves by checking the correct box,"* Krystlik notes. *"Large companies often use solutions that automatically detect keywords and encrypt the communication if necessary, or even prevent it from being sent to ensure that it does not leave the company if not permitted by its distribution rules."*

The classification method, meanwhile, may vary from one organisation to another. Where such a method exists, the Data Protection Officer (DPO) generally sets the framework for the classification, and then it is up to the data producer to determine whether their data is confidential or not. This raises **the issue of digital hygiene**. Before data can be classified in order to protect it or limit its distribution, its owner or producer must first be aware of its value. *"It's a question of paying attention to what you send, and to whom. This is a digital hygiene issue, but it also assumes a certain degree of maturity regarding the data on the company's part, and people need to be trained in this concept and its challenges",* Paffumi notes. It also raises the question of how this knowledge will be maintained. *"Faced with a cyber-topic that we are all still struggling to incorporate into our daily lives, we can see that each year, the company's DPO must provide a reminder of data policy rules."* A time-consuming practice, but an essential one.

The question of maturity also arises when it comes to backup. *"Data backup is a subject that needs to be tackled jointly by different parties,"* Paffumi warns. *"The responsibility for this is shared between the IT department and the business units. The business unit must firstly identify whether it has data that are of value to the company; and secondly, to what extent the destruction, loss or theft of those data may be problematic. It is therefore strongly involved in their protection. Meanwhile, the IT function must be familiar with these data so that it can provide the appropriate tools and infrastructures to help protect them, and deliver the ability to restore them if necessary. The objective is to avoid 'shadow backup' or 'shadow data storage', in cases where business teams implement their own local solution and store their data on a server or a cloud storage solution without the IT or the security team knowing about it."* This is simple on paper, but dramatically complex in reality, especially when shadow IT comes into play...



To conclude, data security is based on an overall approach that combines perimeter protection, workstation protection and data protection. *“There is actually no such thing as unimportant data. This means that there is a real need to provide different layers of protection: firewalls for networks, endpoint solutions for workstations, and encryption or leak prevention solutions for the actual data (Data loss prevention, DLP),”* Paffumi notes. *“And a need to follow a rigorous safeguard policy.”* Lastly, the best option is to plan a Business Recovery Plan (BRP) or a Business Continuity Plan (BCP). And to store it, you are free to print it and keep it in a physically secure space, or keep it in digital format but in a separate and isolated server in order to ensure that it is not itself encrypted!



STORMSHIELD



Stormshield, a wholly-owned subsidiary of Airbus CyberSecurity, offers innovative, end-to-end security solutions for the protection of IT networks (Stormshield Network Security), workstations (Stormshield Endpoint Security) and data (Stormshield Data Security).

www.stormshield.com