LAW FIRMS

Attorneys and lawyers deal with tons of digital information.
Encryption is a law firm's best defense against the violation of their or their clients' privacy. Data breaches, hacking attempts, or embarrassing leaks due to human error are commonplace, and the legal sector is particularly vulnerable due to the highly sensitive client data that lawyers traffic in.

DBV SuperEncryption is helping law firms secure top classified legal documents in an impenetrable and unbreakable way, while making it possible to transfer confidential data between lawyers and their clients.

“I forgot my laptop in the back of a cab” is less dramatic when all contracts are SuperEncrypted on that laptop, and even “my firewall was hacked by a team of nefarious cybercriminals,” does not present a real threat anymore, because data that cannot be read is useless to cybercriminals.

BANKS, FINANCIAL FIRMS AND ACCOUNTANTS

Top secrecy is needed when handling files related to investment portfolios of clients. These can be kept always encrypted, but when you need to work on a file of a client, you then have to ‘decrypt’ the file and this makes your data exposed and vulnerable to hacking.

The DBV SuperEncryption System lets you work on encrypted files without the need to ever decrypt them, therefore reducing to zero the exposure of the clients. Financial institutions employ DBV SuperEncryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit. Communicating restricted financial information to clients, without compromising the data, is made technically feasible by using the DBV System.

HEALTHCARE SECTOR

Electronic health records include insurance information, proper dosage amounts for medicine, and other personal information. The digital age of healthcare allows for easy access to this sensitive information to provide more efficient care. Enhancing healthcare data protection through the use of encryption has become increasingly necessary. Hackers have learned to target providers, like hospitals and clinics, and payers, like plan managers and insurance companies.

Data breaches in healthcare aren’t always attempts to steal information. Some cyber-criminals use ransomware to make quick money from hospitals that desperately need to access information so they can treat patients properly. The DBV Offline SuperEncryption System is immune to any online/remote type of hacking, ransomware, spyware or malware.

GOVERNMENT INSTITUTIONS & ORGANIZATIONS:

Data “at rest” & data “data in transit” poses a growing concern for government institutions which have individuals who access this data through mobile devices, which also exposes database management systems and file servers to more risk in the event these devices are lost or stolen.

DBV SuperEncryption safeguards organization's data and information from potential threats and ensures that even if an intruder gained access to an institution’s sensitive information, it will be unreadable, even if the attack was online or offline, in its physical location. Edward Snowden had the keys to the data he leaked, which highlights the need to consider encryption as part of a broader data protection strategy, and focus on how encryption keys are generated, by whom, how they are managed, where they are stored, and they are used. DBV offers disruptive technologies and innovative solutions for that. Institutions can now completely eliminate cyber-attack threats on their data and information exchanges.

SuperEncryption & Compliance

Nowadays data protection is no longer an option. Companies can’t ignore the problem and hope they won’t be targeted by malicious outsiders. This kind of strategy might have been a viable if risky option in a pre-GDPR world, but since the European Union’s General Data Protection Regulation took the world by storm, there are few countries where data protection legislation has not been adopted or is currently being debated.

The core of these new laws is data protection by design and by default, with the data subject as the focus. Under them, companies can be fined not only for data breaches but also for failing to respect the new rights granted to data subjects under them. Using encryption to protect sensitive data, whether at rest, in transit or on the move, is an effective step towards compliance.

POLITICIANS, JUDGES, JOURNALISTS & HUMAN RIGHT ACTIVISTS

Often VIPs, Celebrities, CEOs, Politicians, Reporters, Dissidents, Activists and more, are a moving target for hackers and are usually victims of personal data leakages, cyber attacks, interception, digital surveillance, tapping and espionage. The DBV SuperEncryption System is offering them an ‘Above Government’ level of encryption and cyber protection.

For newspapers, television companies and similar firms, it is not trade secrets or new innovations that provide value to their business, but the content they produce. This needs to be protected from competitors, but also when it's being shared internally.

BIOTECH , SHIPPING, AUTOMOTIVE & PHARMACEUTICAL

Any business that's involved in high-tech research and development will naturally generate large amounts of data that will be essential to the effective running of the business, scientific research and patenting. In some cases, having confidential intellectual property exposed could even put the entire business in jeopardy.

Whether it's pharmaceuticals, shipping, automotive or technology manufacturing, this data needs to be encrypted any time it is transferred. This includes emails being sent internally, as well as the sharing of data externally, for example with patent offices. Moreover, they need a solution for easily transferring large volumes of data.

ENERGY & UTILITIES

The Energy and Utilities sectors are attractive targets for a special breed of hacker: cyberterrorists. Cybercriminals, sometimes acting on the behalf of foreign nation-states — such as Russia, North Korea, Iran or China. DBV SuperEncryption Technologies prevent the stealing of vital data from this field that is handling sensitive information on a daily basis.