How does the General Data Protection Regulation Affect Industry Data Destruction?

1. **NAID AAA Certification 2.1c requires a company to report a breach in 60 days where the GDPR requires 72-hour notification.**

'2.1c The Company has a written policy in place, stating that the Company will notify any Customer of a potential release of, or unauthorized access to, that Customer's Confidential Customer Media that poses a threat to the security or confidentiality of that information within 60 days of the date of discovery of the data security breach incident.'

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Article 33 1. 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. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. **The companies that perform offsite services which include working in their truck in the parking lot do not conform to industry standards for information security.**

There are several reasons that companies perform offsite or parking lot services is that they use a technology that creates large amounts of e-waste particles and it should not be done onsite. These companies are also staffed sparingly and send one technician to do a job that is mandated to have 2 technicians according to US NIST SP800-88 r1. Then the companies wait many days to hold the hard drives in poorly secured warehouses that would never meet the requirements for any secure datacenter. In the truest words, the data is easy to compromise.

The General Data Protection Regulation 83 and 84 statements are about conducting and accepting risk. When making the analysis, the CISO and Compliance officers measure whether all technologies place data bearing devices in compromised locations and if the data bearing devices are at risk, then the executive officers take the necessary steps to counter the possibility of a breach with insurance to cover the hundreds of millions of dollars of data.

There are companies that do data sanitization inside the four walls of the datacenter, so there is no possible way a risk assessment can accept the notion of offsite data destruction or doing the work in the parking lot inside a vehicle that does not meet the criteria of the facility's datacenter.

83. In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

84. In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

3. **The company creates a new position separate from the CISO called the 'Data Protection Officer'. One of their duties is to perform a risk assessment of the possibility of a data breach from initial concept of the data center to end of life.**

A task of the Data Protection Officer is to examine risk of the data of EU citizen being breached. In a risk assessment, a fictitious Acme Company CISO examines whether to process hard drives onsite and to verify the data sanitization before removing the hard drives. Acme Company examines a company to perform the work onsite that has a sanitizer and verifier and international certifications. The Data Protection Officer scores the risk at the lowest of 1 on a level of 1 to 10 with 10 being the biggest risk, because the hard drives will be destroyed within the four walls of the datacenter. The second company examined sends a single driver to pick up the hard drives. The hard drives are put in the truck and leave the control of Acme Company.

The warehouse where the hard drives are delivered is in a standard city zone where 10 plus robberies occur every 12 months. The warehouse is unguarded 15 hours a day and 24 hours a day over the weekend. The national company has had some history of employees taking hard drives in the last decade. The Data Protection Officer scores the risk at 9 on a level of 1 to 10 with 10 being the biggest risk, since the hard drives will be out of the control of the company for 2 months before they are destroyed and there is no real evidence that the hard drives are actually destroyed. In 2016, the US Government ruled in a patent action that a video of the data destruction for verification is not valid.

The offsite data destruction company is about to lose their contract, so they offer to do the work in the parking lot with their shredding machine. The Data Protection Officer scores the risk at 8 on a level of 1 to 10 with 10 being the biggest risk, since the hard drives will be out of the control of the company's datacenter and there is only one worker when industry standard (NIST SP800-88r1) requires two to counter collusion. There also is a requirement for verification of the work by sampling or another method, which the shredder does not have one. The company that has given them 'Certificate of Destruction' for the last three years and it has been found that the certificate does not meet the NIST SP800-88r1 standard which it is defined by showing that the company is professionally negligent of understanding their industry's regulation. Basically, the data destruction company has always sided with economy and to maximize its profits and not to show respect for data security.

The Data Protection Officer determines that the information on the hard drives is valued at nearly 250 million dollars and the cyber security insurance will not accept the risk of offsite date destruction.

This is just a scenario that the Data Protection Officer would help the CISO make decisions about risk.

(76) The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment; by which it is established whether data processing operations involve a risk or a high risk.

(77) Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

4. **The company starts to track hard drives using RFID tags or active Beacons because once they are removed from the Storage Server or they have failed, they no longer communicate with the management system of the Storage Server. A large company with a large datacenter has the capacity to track physical devices using technology that will allow for regular inventory of critical assets.**

(78) The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders.

5. **The company has to rewrite the contract with the data destruction company to include the requirements of the General Data Protection Regulation. If the new 'Data Protection Officer' has already examined previous year 'Certificate of Destruction' and associated data and found that the company's information is not compliant, or if the risk assessment shows that historically the company jeopardized data, the contract should be awarded to a company that will meet the General Data Protection Regulation.**

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data

subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

6. **The company choice to jeopardize the processing of data bearing devices outside the datacenter in a warehouse or in the parking lot without equal security measures and to regulations that have been in existence for over 24 months has shown to accept high risk for convenience and without regard to data safety.**

The supervisory authority should respond to reckless abandon of physical security of data bearing devices that is not equal or better than what was provided in the datacenter location. The supervisory authority can suspend activities of a company that is jeopardizing the security of data covered by the General Data Protection Regulation.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(96) A consultation of the supervisory authority should also take place in the course of the preparation of a legislative or regulatory measure which provides for the processing of personal data, in order to ensure compliance of the intended processing with this Regulation and in particular to mitigate the risk involved for the data subject.