DATA PROTECTION & DATA SECURITY

Deutsche Industrie Video System GmbH (DIVIS)

White paper, October 2018

DIVIS
THE INTELLIGENT VIEW

READY FOR BUSINESS WITH DIVIS SOLUTIONS

On May 25, 2018, the EU GDPR became effective.

GDPR

The purpose of the regulation is to protect the rights of natural persons with regard to collection and processing of their personal data. For this reason, the regulation defines corporate responsibilities and information requirements on the use of personal data collected. Also regulated is the protection of the collected data against manipulation, loss, disclosure to third parties and misuse by organizational and technical means. Affected persons also receive the legally anchored right for disclosure about storage and processing of their personal data and thus an opportunity to look into this process and take control of it.

The EU GDPR and other new national data protection laws, which are intended to regulate the situation in a concretized manner, have sparked uncertainty and confusion in many companies, because despite the general information flow around May 25, 2018 many regulations still need to be explained and clarified. Many companies fear disadvantages, rising costs and legal conflicts. Many are still unsure about what measures to take in order to act "DSGVO compliant".

The new legislation has undoubtedly created new challenges. The requirements for transparency, security and protection of data during collection, processing and storage have increased. At the same time, this also opens up the opportunity for companies to optimize their own quality management.

For DIVIS, the legal changes are not really a new challenge, because one of the most important features of our system solutions has long been the high level of data protection and data security. As an experienced IT provider, we are aware of the delicate issue of data security not only since the introduction of the EU GDPR. For 15 years, we have been developing and selling turnkey system solutions for visual consignment tracking in freight forwarding and package handling as well as in transshipment warehouse logistics. Our systems are in operation at more than 400 locations and in 19 European countries.

In this white paper we show you how the use of well thought-out products goes hand in hand with a high level of data security and effective work and how your quality management can benefit from it. Learn more about how DIVIS products can help you tailor your video surveillance system to today's and tomorrow's needs without sacrificing targeted video intelligence in your organization using the solution and security approach of DIVIS products.

DATA PROTECTION AND DATA SECURITY AT DIVIS

DIVIS' video surveillance software addresses data protection and data security issues with a number of features and solutions:

MASKING OF PRIVATE AREAS

Our video system solutions allow the targeted obscuring (blurring) of individual image areas, for example, to protect the personal rights of employees.
If a workstation has to be hidden in a specific area or if processes are only to be observed in partial areas of an image, this is possible with DIVIS software.
In the outdoor area, for example, adjacent public areas can be masked.

AUTHENTICATION USING THE FOUR-EYE PRINCIPLE

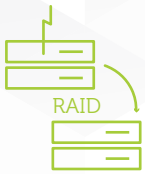
The password function in the DIVIS software ensures that an evaluation of images can only be performed by authorized persons. It is also possible to protect access to the data via a 4-eye password function. The reproduction and evaluation of recordings are only possible with the consent of two persons, by entering their personal password.

USER AND GROUP ACCESS

The software solutions of DIVIS contain a comprehensive role/rights concept for different users. Depending on the required data protection level, a specific, previously defined group of persons as well as individual users with individual access and administration rights can be created. In this way, it is possible to define who will receive access to devices and data to what extent down to the level of individual video systems.

EVIDENTIAL RECORDINGS IN LEGAL DISPUTES

DIVIS video surveillance systems strengthen your evidence situation with customers and partners and, in the event of legal disputes, meet all requirements regarding image quality, tamper-proof and third-party access that are mandatory for evidence material used in a law suit.



FAILOVER AND REDUNDANCY MECHANISMS

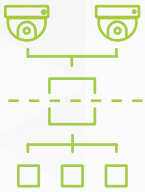
If hard disks fail in the DIVIS video system, a RAID (= redundant arrangement of independent hard disks) intercepts the fault. This guarantees trouble-free long-term operation during simultaneous failure of up to two hard disks.

The data is redundantly protected by the RAID. In the case of a hard disk failure, the disk can be replaced and the original state can be restored without loss of data after the failed component has been replaced.

PIXELATION

With our software module Pixel+ all movements can be pixelated in a 1024-raster. This can optionally be applied either to the entire image or only to partial areas.

With another function, the manual blackening of image areas in which, for example, an employee could be recognized, is also possible. This ensures that in the daily communication (operative system use) no data protection critical information is inadvertently forwarded to third parties.



SEPARATE CAMERA NETWORK

In addition to the customer's operative network, we are building our own, autonomously operating network solely for the DIVIS video system in order to rule out interferences between the networks due to technical influences as far as possible and to avoid manipulation in the best possible way.

LOG FILE PROTOCOL

All activities in the DIVIS video surveillance software are logged using log files. The log history not only provides important information about the operations that take place in the background, the search numbers, or the logs of other users. The log files can also play an important role in legal disputes and have decisive evidential value.

DEFINABLE RESEARCH TIME WINDOW

Due to the extensive user management in the DIVIS software, the access to video recordings for the various user groups can be limited in time. The limitation of the search time window can refer to both the scan time and as well as a selected period of time. Camera images that are older than the set period can not be viewed or evaluated.

STORAGE AND AVAILABILITY OF THE DATA

Our video surveillance systems are equipped with a digital ring buffer. According to your preferences we can individually adjust in the settings of the recorders how long the ring buffer should hold the data. The ring buffer method allows for the data to be stored continuously and be overwritten after the expiry of the specified period of time. As a result statutory provisions for limited data storage can also be met.

FURTHER LEGAL REQUIREMENTS

As a consequence of the EU GDPR further legal requirements have arisen or tightened, which are crucial for companies:

MANDATORY INFORMATION ON SITE

Companies with video surveillance in use are subject to various additional regulations regarding "identification obligations". The new information requirements for non-public places using video surveillance are regulated in Article 13 of the GDPR and are binding.

For our customers, we have created free print templates for the mandatory signage regarding video surveillance, which we will gladly send you on demand. Further information can be found here: https://www.divis.eu/en/gdpr-expands-information-requirement-for-video-surveillance-in-non-public-areas/

PRIVACY ASSESSMENT AND DATA PROTECTION OFFICER

Last but not least, the EU GDPR also defines the specifications for the appointment of a data protection officer. Companies should take action regarding this matter. Companies with more than 10 employees are required to appoint a data protection officer for the purposes of the data protection impact assessment.

The data protection impact assessment represents a prior check-up for which the data protection officer is responsible under the law. According to Art. 35 (1) GDPR, this must always be carried out when particularly sensitive data are processed, for example "if a form of processing is likely to entail a high risk to personal rights and freedoms because of the nature, scope, circumstances and purposes of the processing, in particular if new technologies are used".

For this reason, we strongly recommend that you consult with your data protection officer or a legal specialist in this area for all data protection issues and have the video concept discussed with you checked.

As a provider of video solutions, we support you comprehensively within our capabilities. However, given the complex legal situation, we can not guarantee that the system you operate and the data you collect comply with all the requirements of the new data protection law. We are also prohibited from giving our own legal advice by the provisions of the Legal Advice Act and legal advice is not part of our performance target.

Decisions which may affect data protection should therefore always be discussed with and examined by a suitable professional.