



PROTECTION & SÉCURITÉ DES DONNÉES

Deutsche Industrie Video System GmbH (DIVIS)

Livre blanc, octobre 2018



DIVIS
THE INTELLIGENT VIEW

SOYEZ PARFAITEMENT ÉQUIPÉ AVEC LES SOLUTIONS DIVIS



Le 25 mai 2018, le RGPD de l'UE est entré en vigueur.

L'objectif du règlement est de protéger les droits des personnes physiques en ce qui concerne la collecte et le traitement de leurs données personnelles. C'est la raison pour laquelle le règlement prévoit des responsabilités contraignantes pour les entreprises et l'obligation de fournir des informations sur l'utilisation des données à caractère personnel qui ont été collectées. En outre, il s'agit également de protéger les données collectées contre la manipulation, la perte, la divulgation à des tiers et l'utilisation abusive par des moyens organisationnels et techniques appropriés.

Les personnes concernées bénéficient également d'un droit légal d'accès au stockage et au traitement de leurs données à caractère personnel et donc de la possibilité d'examiner et de contrôler ce processus.

Le RGPD de l'UE et d'autres nouvelles lois nationales relatives à la protection des données, qui visent à réglementer la situation de manière plus détaillée, ont suscité des interrogations et des troubles dans beaucoup d'entreprises, car de nombreuses réglementations doivent encore être expliquées et clarifiées malgré le flux important d'informations qui ont circulé dans la semaine du 25 mai 2018. Certaines entreprises redoutent les désavantages, l'augmentation des coûts et les conflits juridiques. Nombreuses sont celles qui ne savent pas encore quelles mesures

doivent être prises pour agir « en conformité avec le RGPD ».

La nouvelle législation a sans aucun doute créé de nouveaux défis. Les exigences en matière de transparence, de sécurité et de protection des données lors de la collecte, du traitement et du stockage ont augmenté. Dans le même temps, cela permet également aux entreprises d'optimiser leur propre gestion de la qualité.

Pour DIVIS, les modifications légales ne constituent pas un nouveau défi, car l'une des caractéristiques les plus importantes de nos solutions système est depuis longtemps le niveau élevé de protection et de sécurité des données. En tant que fournisseur informatique expérimenté, il n'a pas fallu attendre la mise en place du RGPD de l'EU pour être conscient de la nature explosive de la sécurité des données. Depuis 15 ans, nous développons et vendons des solutions système clés en main pour le vidéotracking, aussi bien dans l'expédition de fret et la manutention de colis que dans la logistique d'entrepôt dans toute l'Europe. Nos systèmes sont opérationnels sur plus de 400 sites et dans 19 pays européens.

Dans ce livre blanc, nous vous montrons comment un haut degré de sécurité des données et un travail efficace vont de pair avec l'utilisation de produits innovants et comment votre gestion de la qualité en bénéficie. Découvrez comment la solution et l'approche de sécurité des produits DIVIS peuvent vous aider à adapter votre système de vidéosurveillance aux exigences actuelles et futures sans pour autant remettre en question la reconnaissance vidéo ciblée dans votre entreprise.

PROTECTION ET SÉCURITÉ DES DONNÉES CHEZ DIVIS

Les logiciels de vidéosurveillance de DIVIS prennent en compte la protection et la sécurité des données grâce à une gamme de fonctionnalités et de solutions :



MASQUAGE DE ZONES PRIVÉES

Nos solutions de systèmes vidéo permettent la pixellisation ciblée (ce qui permet de rendre méconnaissables) des zones d'image individuelles, par exemple pour protéger les droits personnels des collaborateurs. Le logiciel DIVIS permet de masquer spécifiquement un poste de travail dans une zone ou d'observer des processus uniquement dans des zones partielles d'une image. Par exemple, les zones publiques adjacentes peuvent également être masquées à l'extérieur.



AUTHENTIFICATION SELON LE « PRINCIPE DES QUATRE YEUX »

La fonction Mot de passe du logiciel DIVIS garantit que les images ne peuvent être évaluées que par des personnes autorisées. Il est également possible de protéger l'accès aux données par un mot de passe selon le « principe des 4 yeux ». La reproduction et l'exploitation des enregistrements ne sont possibles qu'avec le consentement de deux personnes, elles doivent pour ceci entrer leur mot de passe personnel.



AUTORISATIONS D'UTILISATEUR ET DE GROUPE

Les solutions logicielles DIVIS contiennent un concept complet de rôles/droits pour différents utilisateurs. En fonction du niveau de protection des données requis, il est possible de créer à la fois un groupe spécifique prédéfini de personnes au préalable ainsi que des utilisateurs individuels disposant de droits d'accès et d'administration personnalisés. De cette façon, il est possible de définir jusqu'au niveau des systèmes vidéo individuels qui a accès aux appareils et aux données et dans quelle envergure.



ENREGISTREMENTS POUVANT ÊTRE UTILISÉS DEVANT LES TRIBUNAUX

Les systèmes de vidéosurveillance DIVIS renforcent le suivi de vos preuves vis-à-vis de vos clients et partenaires et, en cas de litiges juridiques, répondent à toutes les exigences en matière de qualité d'image, d'inviolabilité et de protection contre les accès non autorisés, qui sont soumises à un tribunal pour apporter des preuves.



MÉCANISMES DE BASCULEMENT ET DE REDONDANCE

En cas de panne des disques durs du système vidéo DIVIS, un RAID (= disposition redondante de disques durs indépendants) intercepte la défaillance. Ceci garantit une utilisation sans problème à long terme pour une défaillance simultanée de deux disques durs au maximum.

Les données sont protégées de manière redondante par le RAID. Si un disque dur tombe en panne, il peut être remplacé de sorte que l'état initial puisse être restauré après avoir remplacé le composant défaillant par une reconstruction et qu'aucune donnée ne soit perdue.



PIXELLISATION

Avec notre module logiciel Pixel+, tous les mouvements peuvent être pixellisés dans une grille de 1024. Ceci peut être appliqué à l'image entière ou uniquement à certaines parties de l'image.

Avec une autre fonction, le noircissement des zones d'image dans lesquelles, par exemple, un employé peut être identifié, est également possible manuellement. Ceci garantit qu'aucune information essentielle sur la protection des données ne soit transmise involontairement à des tiers au cours des échanges quotidiens (utilisation du système opérationnel).



RÉSEAU DE CAMÉRAS SÉPARÉ

Pour les solutions de systèmes vidéo, nous avons mis en place un réseau séparé et autonome pour le seul système vidéo DIVIS, en plus du réseau opérationnel du client, afin d'exclure autant que possible toute interférence mutuelle par des influences techniques et d'éviter autant que possible toute manipulation.



FICHIERS LOG - ENREGISTREMENT

Toutes les activités du logiciel DIVIS pour la vidéosurveillance sont enregistrées dans des fichiers log. L'historique du fichier log fournit non seulement des informations importantes sur les processus qui ont lieu en arrière-plan, les numéros d'envoi recherchés ou les fichiers log des autres utilisateurs. Les fichiers log peuvent également jouer un rôle important en cas de litiges juridiques et avoir une valeur probante décisive.



PÉRIODE DE RECHERCHE LIMITÉE

Grâce à la gestion étendue des utilisateurs dans le logiciel DIVIS, l'accès aux enregistrements vidéo peut être limité dans le temps pour les différents groupes d'utilisateurs. La limitation de la fenêtre de temps de recherche peut se référer à la fois au temps de scannage et à une période sélectionnée. Les images caméra plus anciennes que la période définie ne peuvent pas être visualisées ou évaluées.



STOCKAGE ET DISPONIBILITÉ DES DONNÉES

En fonction de vos besoins, nous pouvons configurer les enregistreurs pour déterminer combien de temps le tampon circulaire numérique dont nos systèmes de vidéosurveillance sont équipés doit conserver les données. Dans la méthode de stockage annulaire, les données sont stockées en continu et écrasées au bout d'une période définie, ce qui permet également de respecter les dispositions légales relatives au stockage limité des données.

AUTRES DISPOSITIONS LÉGALES

Le RGPD de l'UE a créé ou renforcé d'autres exigences légales qui sont décisives pour les entreprises :



INFORMATIONS À FOURNIR LORSQUE DES DONNÉES À CARACTÈRE PERSONNEL SONT COLLECTÉES SUR SITE

Les entreprises qui exploitent des systèmes de vidéosurveillance sont soumises à diverses réglementations supplémentaires concernant l'obligation de présenter une « preuve d'identité ». Les nouvelles obligations d'information pour les organismes non publics sous vidéosurveillance sont réglementées de manière contraignante par l'article 13 du RGPD.

Nous avons créé pour nos clients des modèles d'impression gratuits pour les pancartes de présence vidéo prescrites, que nous vous enverrons volontiers sur demande. Pour de plus amples informations, cliquez ici :

<https://www.divis.eu/fr/le-reglement-dsgvo-en-matiere-de-protection-des-donnees-etend-le-marquage-obligatoire-dans-la-videosurveillance-dans-des-lieux-non-publics/>



ANALYSE D'IMPACT SUR LA PROTECTION DE DONNÉES ET DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Enfin, et c'est un point particulièrement important, le RGPD de l'UE précise également les dispositions relatives à la nomination d'un délégué à la protection des données. C'est là que les entreprises devraient agir de manière indépendante. Les entreprises de plus de 10 salariés sont tenues de désigner un délégué à la protection des données aux fins de l'évaluation de l'impact relatif à la protection des données.

L'analyse d'impact sur la protection des données est un contrôle préalable dont le délégué à la protection des données de l'entreprise est légalement responsable. Selon l'art. 35 par. 1 du RGPD, cela doit en principe toujours être effectué lorsque des données particulièrement sensibles sont traitées, c'est-à-dire « si une forme de traitement, en particulier l'utilisation de nouvelles technologies, est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes en raison de la nature, de la portée, des circonstances et des finalités du traitement ».

C'est pourquoi nous vous recommandons expressément de consulter votre délégué à la protection des données ou un avocat spécialisé dans ce domaine pour toutes les questions relatives à la protection des données et de faire vérifier le concept vidéo avec vous.

En tant que fournisseur de solutions vidéo, nous vous soutenons de manière globale dans la mesure de nos possibilités. Compte tenu de la situation juridique complexe, nous ne pouvons toutefois pas garantir que le système que vous utilisez et le traitement des données collectées sont conformes à toutes les exigences de la nouvelle loi sur la protection des données. Notre propre conseil juridique est également exclu par les exigences de la loi sur le conseil juridique et ne fait pas partie de notre palette de prestations.

Les décisions susceptibles d'affecter la protection des données devraient donc toujours être examinées par un organe approprié.