Welcomr

Contrôle d'accès & RGPD

LIVRE BLANC
JANVIER 2021

#AccèsAuxBâtiments #Bâtiment #Contrôled'accès
#Cloud #SaaS #Habilitations #Traçabilité
#EnvironnementdeTravail
#DonnéesPersonnelles #ViePrivée
#Sécurité #Privacy #Security #CNIL #ANSSI #DSI
#RSSI #DPO #Immobilier #Tertiaire #Industrie #RH
#DroitduTravail #RGPD #LPM #Salariés
#Visiteurs #Sûreté #IntelligenceEconomique
#Cybersécurité #SmartBuilding

SYNTHÈSE MANAGÉRIALE

Le contrôle d'accès physique appelle à des processus qui amènent l'entreprise à manipuler des données sensibles et confidentielles. L'entreprise collecte et traite notamment des données à type d'identité des salariés, des prestataires, des visiteurs, et d'horaires d'entrée et parfois de sortie.

Il nous est alors apparu indispensable que Welcomr soit le premier à proposer un document de référence sur le sujet du RGPD et de son impact sur le contrôle d'accès, puisque la solution SaaS de gestion des accès Welcomr se veut par essence protectrice de la vie privée et sécurisante pour les données dont elle participe au traitement.

Ce livre blanc aborde l'importance de disposer d'un système de contrôle d'accès sécurisé "by design" (de l'anglais : dès la conception), du rôle que la gestion des accès aux bâtiments joue dans la réponse aux exigences de conformité du RGPD, et plus généralement de la nécessité pour les entreprises de garantir à leurs parties prenantes un niveau de confidentialité conforme à l'État de l'Art.

PRÉFACE

“Cloud et RGPD : pour un avantage concurrentiel combiné au service de l’expérience utilisateur.”

Vos données ont une valeur et leur gestion représente un défi qui nécessite de plus en plus l’intégration de nouvelles réglementations et politiques internes à l’entreprise. La montée en puissance des cyberattaques et fraudes en tous genres témoignent du fait que les données sont au cœur des enjeux de l’économie digitale du XXIème siècle.

Actifs immatériels et divers secrets des organismes privés et publics, il ne fait aucun doute que les données doivent être protégées contre les accès frauduleux, les altérations, les suppressions, les modifications, les divulgations, les usurpations, les pertes et les fuites. Toutes les organisations, et particulièrement celles qui gèrent une grande quantité de données personnelles, doivent être préparées à une éventuelle violation de données.

Ainsi, au-delà de la protection des données personnelles, le RGPD protège le capital immatériel des entreprises privées comme des organismes publics. Si les solutions juridiques ont pour but de prévenir et de gérer les risques, l’obligation de moyens est implicite et oblige les différents services de l’entreprise à collaborer et à partager les informations et bonnes pratiques.

Depuis 2012, la “Data Protection by Design” et le “Privacy by Design” ont été incorporés aux réglementations européennes comme étant consubstantiels à l’élaboration des systèmes numériques.

Désormais, la question est aussi de savoir comment sécuriser les données dans un écosystème gouverné par les solutions cloud.

Interagir avec les serveurs doit impérativement se faire par transmission chiffrée SSL (secured socket layer) afin de se doter du meilleur niveau de sécurité possible, tout en bénéficiant de la souplesse du cloud.

Le contrôle d’accès en SaaS permet de protéger physiquement les accès aux données sensibles ainsi qu’à celles des partenaires et visiteurs, dans le respect des directives du RGPD.

Le contrôle d’accès en SaaS peut également devenir un levier de performance au service de votre entreprise en offrant à vos collaborateurs et clients, les garanties nécessaires afin que le traitement que vous mettez en œuvre pour leur compte soit gage de confiance.

Pour toutes ces raisons et ainsi que le vous le démontrera ce livre blanc, il est indéniable que la solution de contrôle d’accès cloud Welcomr allie flexibilité et agilité à tous les niveaux.

Par Agnès Boschet Guichard

DPO, gérante d’ABG-3D, cabinet de conseil en Intelligence stratégique & Business Development, Data & Cybergouvernance.

AU PROGRAMME

Synthèse managériale 03
Préface 05
Au programme 06
Introduction 07

1. POURQUOI LE CONTRÔLE D'ACCÈS DOIT-IL FAIRE L'OBJET D'UNE ATTENTION PARTICULIÈRE EN MATIÈRE DE CONFORMITÉ AU RGPD 10
Rappels sur le RGPD 12
Le contrôle d'accès est générateur de données personnelles 13
Le contrôle d'accès "traditionnel" est une source de risque car il ne répond plus aux exigences de sureté attendue 14

2. LE CONTRÔLE D'ACCÈS EN CLOUD COMME GAGE DE RENFORCEMENT DE LA CONFORMITÉ RGPD ? 16
Rappels sur le RGPD et le SaaS 18
Le RGPD force la convergence entre sécurité physique et sécurité logique 20

3. DE LA CONFORMITÉ RGDP À LA PERFORMANCE DU CONTRÔLE D'ACCÈS AUX BÂTIMENTS 22
La performance, grâce à un contrôle d'accès agile et robuste 24
Qui dit protection des données, dit nécessairement sécurité des données 27

4. UNE FLEXIBILITÉ GARANTIE 28
Aider les entreprises à protéger leurs collaborateurs, leurs données sensibles et leurs visiteurs 30

5. CONCLUSION 32

INTRODUCTION

Depuis le 28 mai 2018, toutes les entreprises implantées sur le territoire européen sont concernées par l'application du Règlement Général sur la Protection des Données (RGPD) et se doivent d'être vigilantes quant au traitement et au stockage des données confidentielles et/ou personnelles.

Le RGPD est venu bouleverser et harmoniser la manipulation des données personnelles.

Pourtant, rares sont les entreprises qui ont agi pour résorber le risque de non conformité de leur système historique de contrôle d'accès aux bâtiments.

Mais le RGDP ne se limite pas aux seules thématiques du traitement informatique et de la cybersécurité.

S'il n'a pas fallu attendre son entrée en vigueur pour que les entreprises protègent l'accès à leurs locaux, cette réglementation européenne insiste également sur la nécessité pour les entreprises d'intégrer le RGPD aux procédures habituelles de contrôle d'accès physique à leurs bureaux.

En effet, pour l'entreprise, sécuriser ses données, c'est aussi sécuriser les accès à ses locaux, et seul un système de contrôle d'accès solide, agile et fiable permet d'éviter les intrusions dans les bureaux ou autres bâtiments de l'entreprise.

Comment le contrôle d'accès en SaaS, sécurisé dès sa conception (by design), permet de protéger physiquement les accès à vos données, à celles de vos partenaires et visiteurs, ainsi que la manière dont cela peut contribuer à améliorer considérablement la performance de votre entreprise ?

Ce livre blanc vise à guider les entreprises dans la mise en conformité de leur gestion des accès physiques avec les exigences du RGPD.

1

POURQUOI LE CONTRÔLE D'ACCÈS DOIT-IL FAIRE L'OBJET D'UNE ATTENTION PARTICULIÈRE EN MATIÈRE DE CONFORMITÉ AU RGPD

RAPPELS SUR LE RGPD

Contexte réglementaire

Promulgué le 25 mai 2018 par la Commission Européenne, le RGPD est aujourd'hui le texte de référence en matière de protection des données personnelles pour les 28 pays membres de l'Union. Remplaçant une directive sur la protection des données personnelles datant de 1995, il s'inscrit dans la continuité de la Loi française "Informatique et Libertés" de 1978 et renforce le contrôle par les particuliers et entreprises européennes de l'utilisation pouvant être faite des données les concernant.

L'objectif du RGPD est de "redonner aux citoyens le contrôle de leurs données personnelles, tout en simplifiant l'environnement réglementaire des organisations". Les différentes dispositions modifient désormais la façon dont les entreprises collectent, gèrent, stockent et protègent les données personnelles de leurs salariés, clients et/ou partenaires.

Périmètre d'action du RGPD

Est tenue de se conformer au RGPD, toute entité appelée de près ou de loin, à manipuler ou traiter des données personnelles à l'échelle européenne, quelle que soit sa taille ou son secteur d'activité ; qu'il s'agisse d'une entreprise privée ou publique, d'un sous-traitant, d'une startup ou bien encore d'une association. A noter que le RGPD concerne par extension les échanges des entreprises européennes avec les pays hors de l'UE, ainsi que chacun de leurs prestataires et sous-traitants.

Ainsi selon la CNIL France, organisme chargé de veiller au bon respect du RGPD, chaque entreprise est tenue de s'y conformer mais aussi de s'assurer que chacun des partenaires avec lesquels elle travaille, met bien en œuvre toutes les mesures nécessaires afin de garantir une protection optimale de leurs données. La protection des données devient un critère indispensable pour choisir ses partenaires comme dans le cas d'un appel d'offres.

Sanctions en cas de non-conformité

En cas de non-conformité, les entreprises qui enfreignent les règles du RGPD encourent jusqu'à vingt millions d'euros d'amende ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent.

À RETENIR

- L'esprit du Règlement Général sur la Protection des Données est de créer un cadre harmonisé afin de forcer la généralisation des bonnes pratiques en matière de protection des données personnelles, en miroir des attentes des citoyens,
- Le RGPD concerne toutes les données personnelles pouvant circuler et être traitées par les entreprises ; on ne compte plus le nombre d'intrusions et de cyberattaques ayant permis de recueillir ces données. Les entreprises sont de plus en plus conscientes de l'importance de sécuriser l'accès à leur(s) bâtiment(s) et à leurs systèmes d'information, et soucieuses d'augmenter le niveau de sûreté et de préservation de la confidentialité,
- Là encore, le contrôle d'accès repose sur des dispositifs de collecte et de traitement de données personnelles et se trouve de facto concerné par le respect de la vie privée des salariés et des visiteurs.

LE CONTRÔLE D'ACCÈS EST GÉNÉRATEUR DE DONNÉES PERSONNELLES

Les accès génèrent de nombreuses données personnelles. Ceci pour tous les types d'usagers des bâtiments : utilisateurs permanents du site, salariés des autres sites de passage sur ce site (dits visiteurs internes), visiteurs des salariés du site, prestataires en régie sur le site, personnels d'entretien et de maintenance du site, etc.

Le gestionnaire du site est investi de plusieurs responsabilités eu égard aux données personnelles d'accès, et notamment de :

- la conformité au RGPD du traitement de ces données personnelles,
- la sécurisation de ces données personnelles vis-à-vis de cyberattaques de tiers externes,
- la minimisation des risques de fuites depuis l'intérieur desdites données personnelles.

Le RGPD, émanation de l'Union Européenne, pose un cadre qui dépasse largement les frontières de l'Union Européenne. En effet, l'initiative et le cadre juridique sont progressivement adaptés dans tous les grands ensembles géopolitiques mondiaux, et dans toutes les démocraties. Ainsi, l'entreprise qui fera lenécessaire pour assurer sa conformité au RGPD se sera naturellement préparée

LE CONTRÔLE D'ACCÈS "TRADITIONNEL" EST UNE SOURCE DE RISQUE CAR IL NE RÉPOND PLUS AUX EXIGENCES DE SÛRETÉ ATTENDUES

Le contrôle d'accès se définit comme le système permettant d'éviter les accès non autorisés et les intrusions dans les locaux de l'entreprise et de sécuriser un ou plusieurs bâtiment(s) :

- Restreindre l'accès à une zone, à un ou plusieurs bâtiment(s), à une salle, ou encore à un service,
- Ouvrir et fermer les portes, barrières et autres points d'accès, par un dispositif électronique et sécurisé,
- Gérer des droits d'accès et des créneaux horaires pour des salles.

Le contrôle d'accès supplante les serrures classiques et leur cylindre mécanique avec différents dispositifs électroniques : béquilles électroniques, lecteurs de badge, lecteurs de codes numériques ou de QR codes, etc. Mais ces dispositifs ainsi que les différentes technologies permettant d'interagir avec ceux-ci (badges RFID, cartes magnétiques, codes, ou encore parfois biométrie) sont d'importants vecteurs de flux de données personnelles et donc de risque.

- Sur chacun des sites, les administrateurs des serveurs ont régulièrement accès à un très grand nombre de données et d'informations. Sans compter que les registres d'accueil visiteurs sont régulièrement gérés par des prestataires, dépositaires du risque de conformité en matière de RGPD,
- La présence en local des bases de données d'accès horodatés et l'encadrement des accès à ces locaux peuvent constituer des failles de sécurité et donc de conformité au RGPD.

Pour rappel, le système de contrôle d'accès ne doit en aucun cas servir de pointeuse et tracer les allers et venues des salariés - l'horodatage n'étant pas l'objet du contrôle d'accès dont la raison d'être est de gérer les autorisations de passage dans un bâtiment.

Dans le cas d'environnements multi sites, l'harmonisation des pratiques d'un site à l'autre est vivement conseillée pour maîtriser ses coûts de gestion des accès, et pour améliorer la qualité de la vie au travail de ses salariés nomades aussi appelés visiteurs internes.

Saviez-vous qu'en cas de contrôle de la CNIL, l'entreprise s'expose à une amende si le logiciel de gestion des accès aux bâtiments affiche des données personnelles à des personnes non habilitées par le consentement individuel des salariés ?

2

LE CONTRÔLE D'ACCÈS EN CLOUD COMME GAGE DE RENFORCEMENT DE LA CONFORMITÉ RGPD ?

RAPPELS SUR RGPD ET LE SAAS

Comment s'assurer de la conformité de son système de contrôle d'accès ?

La sécurité et la protection de la vie privée sont des questions primordiales. Si un fournisseur de services subit une atteinte à la protection des données, cela peut potentiellement compromettre toute la sécurité des données de l'entreprise et la disponibilité de ses services.

Le contrôle d'accès en cloud permet aujourd'hui de renforcer grandement la conformité au RGPD. La gestion du contrôle d'accès en cloud ou en mode SaaS présente de multiples avantages et offre la possibilité de :

- Améliorer la performance et la qualité du travail du service d'accueil grâce à la préparation des visites en amont,
- Alléger la charge de travail des collaborateurs en leur permettant de préenregistrer et de valider les visites grâce aux règles métier de Welcomr,
- Diminuer le temps d'attente des visiteurs à l'accueil,
- Limiter les risques de piratage ou de dommage aux installations en intégrant les visiteurs dans le système de contrôle d'accès,
- Assurer la traçabilité des visites en cas d'audit ou de contrôle d'un organisme de certification.

Accessible sur le cloud, une application en mode SaaS de gestion des accès évite aux entreprises de devoir sécuriser des serveurs en local sur chaque bâtiment et de créer des réseaux privés virtuels de chaque bâtiment vers un serveur central.

Chez Welcomr, on parle de sécurité "by design" pour qualifier l'externalisation des applications de gestion des accès ; à savoir que les innovations intégrées dans un ensemble de mises à jour ainsi que le maintien d'un haut niveau de sécurité dans l'hébergement sont réalisées en continu et font partie intégrante du service rendu aux clients.

Le recours à l'installation d'un dispositif de contrôle d'accès en SaaS doit faire l'objet d'un engagement de conformité déposé auprès de la Commission Nationale Informatique et Libertés (CNIL).

Cet engagement de conformité doit répondre à la norme simplifiée NS-042, qui concerne la gestion des contrôles d'accès (non biométriques) sur les lieux de travail pour les salariés et les visiteurs, la gestion des horaires ainsi que la gestion de la restauration.

L'employeur se doit ainsi d'informer ou de consulter les instances représentatives du personnel, avant de décider d'installer un dispositif de contrôle des accès.

Il ne doit également pas oublier de communiquer à chaque salarié les informations relatives aux finalités poursuivies, aux modalités de fonctionnement du système dans sa globalité et aux destinataires amenés à disposer des données gérées par le système de contrôle d'accès. La communication de ces différentes informations peut, à titre d'exemple, se faire par une simple note de service, ou bien par un avenant au contrat de travail.

A noter que le salarié est quant à lui en droit de faire état de son opposition pour motif légitime et bénéficie d'un droit d'accès aux données le concernant et peut en demander l'effacement. Il dispose également d'un droit de rectification et d'un droit à la limitation du traitement de ses données.

À RETENIR

- Dans le RGPD, le législateur avait intégré la démocratisation du cloud computing. Ainsi, la gestion du contrôle d'accès en cloud, ou en mode SaaS, répond totalement au cahier des charges du RGPD en tant que solution sécurisée by design.

"La protection des données : une condition sine qua non à l'amélioration du service et de l'expérience utilisateur"

L'avis d'expert de Louis Paumier,
Secrétaire Général de la société française MonBuilding, éditeur de solution SaaS pour la gestion immobilière

La protection des données : une condition sine qua non à l'amélioration du service et de l'expérience utilisateur

Les données personnelles sont désormais au cœur des préoccupations des utilisateurs et des services généraux des entreprises.

Il est impensable aujourd'hui de ne pas tenir compte de ces enjeux dans le choix d'une solution de gestion des immeubles – et en particulier de tenant experience software, dans lequel la donnée des utilisateurs est centrale. Les utilisateurs doivent être assurés que leurs données sont protégées et resteront confidentielles.

Le législateur français s'est intéressé très tôt à ces problématiques, les autres États européens lui ont progressivement emboîté le pas jusqu'à la mise en place du RGPD et ce n'est qu'aujourd'hui que les autorités américaines commencent réellement à s'en préoccuper. Ce décalage culturel se retrouve dans l'approche de la protection des données par les différents éditeurs de solutions, dont la sensibilité est très souvent liée à leur pays d'origine.

Afin de se conformer à la réglementation applicable et aux attentes des utilisateurs, il convient de choisir une solution conçue autour des principes de privacy by design et de privacy by default. En pratique, la solution retenue devra être sécurisée, ne traiter que les données personnelles nécessaires à son fonctionnement, être hébergée en Union Européenne, dans l'Espace Economique Européen (EEE) ou dans un des rares pays reconnus "adéquats", et permettre aux utilisateurs d'exercer effectivement leurs droits.

Cela peut sembler une contrainte, en réalité c'est une opportunité. Encadrer l'utilisation des données, c'est garantir qu'elles ne sont traitées que pour que l'application remplisse son rôle : améliorer l'expérience utilisateur et la qualité du service au sein de l'immeuble.

LE RGPD FORCE LA CONVERGENCE ENTRE SÉCURITÉ PHYSIQUE ET SÉCURITÉ LOGIQUE

Le cloud permet d'empêcher un assaillant d'exploiter une faille ou de contourner le système de sûreté cyber ou physique du contrôle d'accès.

En effet, en cas de compromission physique, un bâtiment disposant de son propre serveur de contrôle d'accès en local qualifierait automatiquement l'accès à son serveur de gestion des accès compromis.

A l'inverse, en cas de compromission logique de l'infrastructure du client, il est difficile de prouver que les applicatifs de gestion des accès physiques n'eussent pas fait l'objet d'une intrusion par la même occasion, déclenchant un risque de faille sur les bâtiments de l'entité visée.

Dès lors, séparer les infrastructures physique et logique permet de renforcer le niveau de sûreté globale d'une entreprise : en cas de compromission physique ou logique du réseau de l'entreprise, le contrôle d'accès physique aux bâtiments est préservé car indépendant.

Réciproquement, en cas de compromission du contrôle d'accès physique, externalisé, le réseau de l'entreprise n'est pas impacté, et donc le patrimoine de données de l'entreprise est préservé.

À l'échelle de toute l'entreprise, le contrôle d'accès en SaaS permet de forcer l'harmonisation des pratiques de traitement des données personnelles

Dans un environnement multisite, le cloud est un gage de réduction des risques de non-conformité.

En effet, le coût de la mise en conformité, et donc le risque de non-conformité, dans un environnement multisite hétérogène sont à multiplier par le nombre de sites. Et surtout, la vie de l'entreprise (fusions, acquisitions, cessions,...) en fait un projet perpétuel.

3

DE LA CONFORMITÉ RGPD À LA PERFORMANCE DU CONTRÔLE D' ACCÈS AUX BÂTIMENTS

LA PERFORMANCE, GRÂCE À UN CONTRÔLE D'ACCÈS AGILE ET ROBUSTE

Au-delà de la conformité, un contrôle d'accès garant de la confidentialité des données contribue directement à l'augmentation de la performance en entreprise pour les motivations suivantes.

Une motivation sociale

Pour les collaborateurs, évoluer dans un environnement agréable et sécurisé est gage d'épanouissement et favorise un climat de confiance qui transparaît également au niveau des partenaires et clients potentiels. L'entreprise apparaît ainsi comme étant une structure fiable et sûre.

Une motivation concurrentielle

Bien qu'elles n'en aient pas toujours conscience, les entreprises détiennent de nombreuses informations dont la valeur économique et stratégique constitue le capital immatériel. C'est ce capital qui, dans un contexte fort concurrentiel, permet à l'entreprise de maintenir sa différenciation et de préserver sa réputation.

Les entreprises doivent se tourner vers des systèmes qui ont été pensés pour la performance et la sûreté "by design"

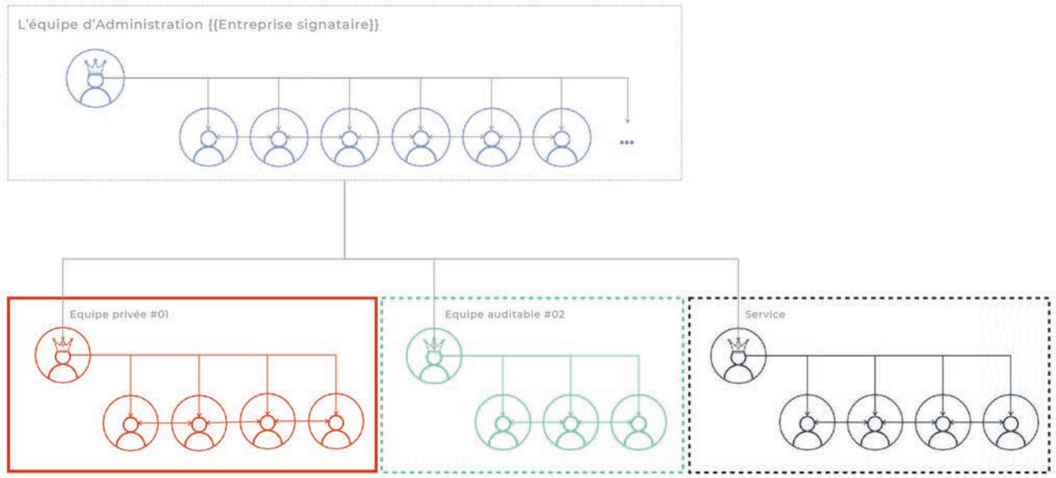
Parce que le contrôle d'accès génère et traite des données confidentielles, il est d'autant plus important pour une entreprise de se tourner vers des systèmes de contrôle d'accès conçus avec la robustesse nécessaire à la sûreté des systèmes et des flux d'informations.

Une gestion des habilitations par couches ou strates

Le contrôle d'accès permet en effet une gestion structurée des droits d'accès, selon laquelle le gestionnaire du ou des lieu(x) ou bâtiment(s), a la possibilité de déléguer tout ou partie de la gestion des droits d'accès à certains de ses locataires, alors désignés responsables de leur propre équipe privée.

Une telle structure est construite de sorte à ce que le gestionnaire n'ait pas accès à la liste des utilisateurs du locataire, qui est confidentielle et réservée à l'usage de l'entreprise locataire.

À noter qu'en cas d'urgence et après en avoir avisé explicitement le locataire, le gestionnaire peut toutefois avoir la possibilité de la consulter. Le locataire qui disposerait d'un tel compte "auditable" est alors notifié de la consultation de son compte par son gestionnaire.



Exemple d'organisation par équipes dans le fonctionnel Welcomr

Ce schéma montre que chaque utilisateur peut voir et agir sur les membres de son équipe et les responsables d'équipes "de niveau inférieur" uniquement.

En aucun cas, un utilisateur n'a accès aux "niveaux supérieurs", ou aux informations des autres équipes de son niveau, sauf si l'équipe a été spécifiée comme auditable à sa création.

Une chaîne de responsabilités claire pour une meilleure traçabilité

Le fonctionnement en équipes, avec des responsables clairement identifiés et disposant des droits d'administration, par délégation du gestionnaire, permet notamment une traçabilité précise de la chaîne de responsabilités. En cas de problème, il est en effet très simple de remonter à la personne en charge et de voir qui doit être tenu responsable de l'incident survenu.

La nécessité de savoir ce que l'on cherche pour réaliser un export

Dans le cas d'un export de données ou d'historique d'accès, la mise en place d'un système de filtres permet de n'exporter et de ne traiter que les données dont a besoin la personne à l'initiative de l'export. La sélection de plusieurs jeux de filtres prédéfinis permet ainsi un traitement par lot optimisé, simple et rapide, tout en garantissant une sécurité optimale des données confidentielles.

Les visiteurs ; une question épineuse résolue

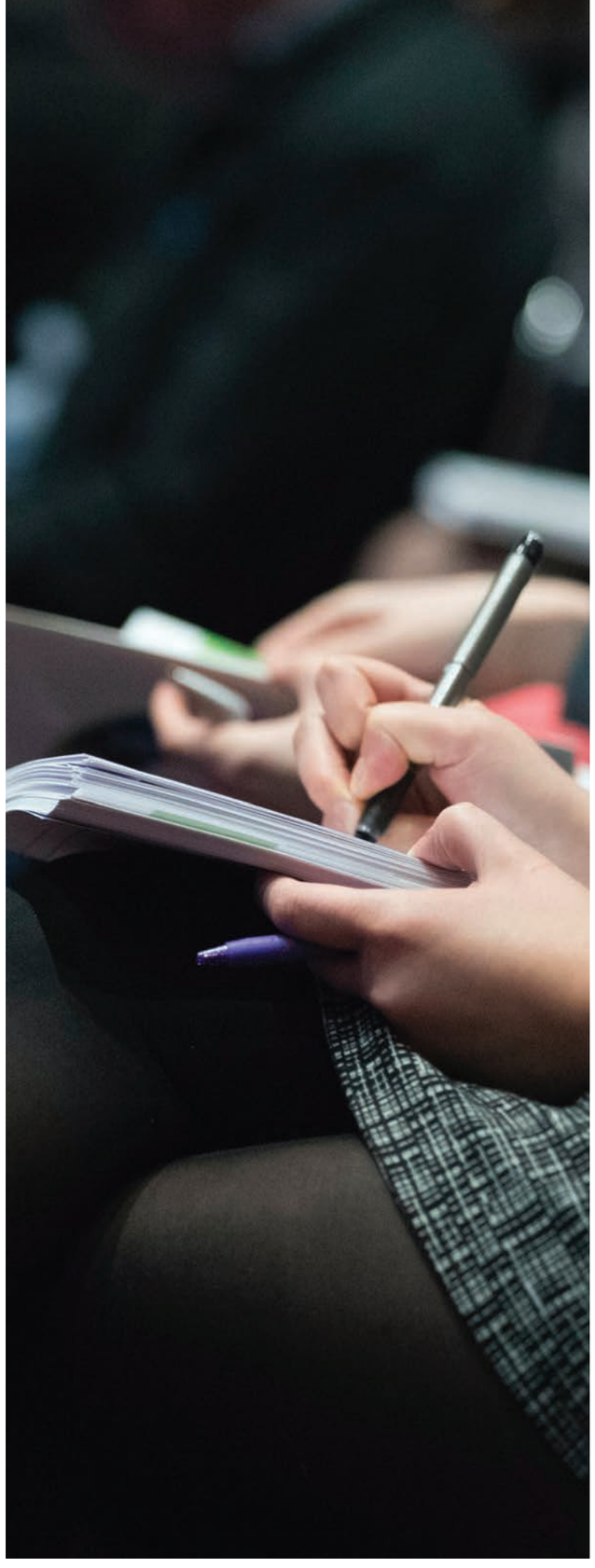
La liste des visiteurs d'une entreprise est peut-être l'un des types de données les plus sensibles. En effet, la liste des visiteurs est le révélateur des talents et cibles de l'entreprise : fournisseurs, clients, partenaires, et de bien d'autres secrets.

Cependant, cette liste est confiée à des prestataires extérieurs, chargés de l'accueil. Il est donc indispensable que le logiciel de gestion des accès sache

encadrer ce processus de sécurisation de ces informations vitales en ne permettant aucun export, en ne permettant pas au personnel d'accueil d'accéder à l'historique des passages, et en garantissant que seules les informations strictement nécessaires fassent l'objet d'un affichage, c'est-à-dire quel visiteur visite quel permanent et sur quel créneau horaire.

À RETENIR

- Au travers de la conception des règles de gestion des accès du Security Center, le nom de son application logicielle, Welcomr assure une préservation des données privées sans précédent. C'est la notion de "Privacy by Design".



QUI DIT PROTECTION DES DONNÉES, DIT NÉCESSAIREMENT SÉCURITÉ DES DONNÉES, À PENSER DÈS LA CONCEPTION

Sécurité physique

Une architecture décentralisée pour protéger le patrimoine de données de l'entreprise constitue l'essence du contrôle d'accès.

Traditionnellement et le plus souvent, les systèmes de contrôle d'accès proposés sont dits centralisés, c'est-à-dire que plusieurs portes peuvent être reliées à un seul et même serveur qui stocke tous les droits d'accès et donc toutes les données privées qui sont liées. Mais ces systèmes présentent une faille de sécurité majeure tant il est aisé de recueillir l'intégralité des données traitées une fois le serveur principal piraté.

Ce n'est pas le cas pour le système de contrôle d'accès Welcomr qui est conçu autour d'une architecture décentralisée. Cela signifie que chaque point d'accès définit, dispose sur le plan matériel de son propre équipement et est totalement indépendant de l'autre. Sur le plan logiciel et en cas de besoin, l'indisponibilité d'un administrateur n'empêche toutefois pas un autre administrateur de gérer les autorisations d'accès.

Sécurité logique

Le contrôle d'accès traditionnel entraîne un enchaînement de technologies variées : un lecteur sera relié à une unité de traitement locale (UTL), qui elle-même sera connectée au serveur disposant du logiciel de gestion des accès en local.

La programmation de ces dispositifs, qui souvent sont issus de plusieurs fabricants (lecteurs, centrales, encodeurs, badges) et éditeurs (firmware, logiciel de gestion des accès des permanents, logiciel d'accueil des visiteurs), nécessite des compétences très pointues dont tous les installateurs ne disposent pas forcément à demeure de manière exhaustive. Ce qui entraîne un nivellement du niveau de sécurité par le bas.

Welcomr, qui est à la fois fabricant et éditeur et donc qui propose une architecture différente et intégrée verticalement, ne risque pas de voir un installateur dégrader le niveau de sécurité prévu car le matériel est préconfiguré pour fonctionner sans programmation spécifique, et le logiciel n'est pas paramétré en local mais configuré à distance suivant le cahier des charges de mise en service et les contraintes de sécurité comme de sûreté du client.

À RETENIR

- C'est la combinaison du "Privacy by Design" et du "Security by Design" qui crée les conditions de la performance en matière de respect de la vie privée,
- Ceci est particulièrement vrai en matière de contrôle d'accès et de gestion des autorisations aux bâtiments, où les risques sont plus nombreux qu'ailleurs en raison du caractère sensible des données traitées,
- L'architecture du contrôle d'accès décentralisé Welcomr présente un niveau de sûreté plus élevé que les architectures traditionnellement centralisées dont le point névralgique constitue une vulnérabilité majeure pour toute entreprise se tournant vers ce type de contrôle d'accès.

4

UNE FLEXIBILITÉ GARANTIE

AIDER LES ENTREPRISES

Les seules données stockées par Welcomr sont le nom, le prénom et l'adresse email de l'utilisateur. Welcomr ne permet pas que les champs de recherche de l'historique horodaté du contrôle d'accès soient utilisés à des fins de traçabilité des individus.

Ainsi, outre le RGPD, Welcomr apporte, de par la manière dont est conçue la solution, des garanties de flexibilité conformes au respect de la vie privée des collaborateurs de l'entreprise :

Aider les entreprises à protéger leurs collaborateurs

L'employeur doit prévoir des mesures pour assurer la sécurité des informations concernant ses salariés et éviter que des personnes qui n'ont pas qualité pour y accéder puissent en prendre connaissance. La solution Welcomr procure une sécurisation des échanges et une journalisation des accès aux données et opérations effectuées en mode SaaS.

Le traitement de la conformité au RGPD est synergétique avec l'intégration d'autres référentiels normatifs tels que la Loi sur la Programmation Militaire ou encore les réglementations applicables aux Établissements Recevant du Public.

Aider les entreprises à protéger leurs données sensibles ; références à la Loi de Programmation Militaire (LPM)

Les Opérateurs d'Importance Vitale (OIV) sont quant à eux tenus de se conformer à la Loi de Programmation Militaire (LPM) qui exige la mise en place de mesures techniques et organisationnelles spécifiques afin de protéger les données sensibles des Systèmes d'Information d'Importance Vitale (SIIV) de ces derniers. Cette loi fait suite à l'implication de l'État pour anticiper et contrer les impacts des cybermenaces présentes et à venir, à l'échelle du territoire national.

L'enjeu principal est de garantir tant la protection des individus que celle des biens et de se prémunir contre d'éventuelles cyberattaques. Les articles 21, 22, 23 et 24 de la Loi de Programmation Militaire (LPM) visent par exemple à améliorer la défense des OIV et imposent le renforcement des règles de sécurité des SIIV utilisés. L'article 13 stipule quant à lui le droit des services du renseignement intérieur de police et de gendarmerie, d'accéder aux données téléphoniques et numériques, dans le cadre notamment de la lutte contre le terrorisme et la criminalité organisée.

Le système de contrôle d'accès Welcomr est pensé "by design" dans l'optique de limiter l'accès aux données personnelles et permet de répondre à ce besoin de conformité. Les données utilisées par la solution Welcomr sont cryptées à la fois "at rest" (en phase de stockage) et "in transit" (lorsque communiquées entre les composants du système).

Le cryptage fait appel à un protocole d'authentification forte à clés diversifiées pour une protection maximale des données personnelles. Si les données privées ne sont en aucun cas recueillies ou traitées par Welcomr et sont à la discrétion de l'administrateur responsable de sa propre équipe, une fonctionnalité permet, en cas d'urgence et à la demande des forces de l'ordre ou compte tenu de certaines directives, de générer un historique des accès et de connaître l'identité chiffrée de la personne ayant pénétré les lieux à un moment donné.

Aider les entreprises à protéger leurs visiteurs ; le cas des Établissements recevant du public à partir d'une certaine catégorie, et des Immeubles de Grande Hauteur

Pour rappel et d'après la définition qu'en donne le Service Public, "les établissements recevant du public (ERP) sont des bâtiments dans lesquels des personnes extérieures sont admises ; que l'accès soit payant ou gratuit, libre, restreint ou sur invitation. Il est à noter que "les ERP sont classés en catégories qui définissent les exigences réglementaires applicables (type d'autorisation de travaux ou règles de sécurité par exemple) en fonction des risques."

Pour certains ERP comme pour les IGH (Immeubles de Grande Hauteur), les règles de sécurité nécessitent de connaître en temps réel le taux d'occupation du bâtiment, certains quotas ne devant en aucun cas être dépassés. Ceci se traduit par la présence, en entrée et en sortie, de portiques automatiques ou Portillons Non Gardiennés (PNG), permettant un comptage des personnes présentes et dans le respect de leur anonymat.

Plus spécifiquement, la liste des personnes, salariés comme visiteurs ou prestataires, présentes sur les lieux à un moment donné peut être exigée. Ce serait le cas par exemple du système d'alerte incendie qui se déclencherait et qui nécessiterait de générer une liste de présence. Le module d'accueil des visiteurs de la solution Welcomr permet, dans ce contexte, de générer la liste des visiteurs présents sur site au moment de l'incident.

À RETENIR

- Le contrôle d'accès a pour double objectif d'augmenter la sûreté des bâtiments et la sécurité de leurs occupants en facilitant l'administration du fonctionnement des accès tout en garantissant la traçabilité des flux.
- La solution Welcomr est robuste (la sûreté de ses systèmes repose sur les notions de Security by Design et de Privacy by Design) et permet d'établir un nouvel État de l'Art en matière de sécurité des données pour le contrôle d'accès.

5

CONCLUSION

Welcomr
est l'alternative éthique pour les entreprises qui ne cherchent aucun compromis entre protection des données personnelles et de sécurité pour leur contrôle des accès.

"Parce que les locaux professionnels ne sont pas ouverts à tous et que les employeurs comme les employés ont besoin de connaître les horaires effectués, les contrôles d'accès et du temps de travail existent depuis bien longtemps.

Le développement des technologies facilite ces contrôles, mais permet aussi de collecter bien plus d'informations sur les personnes concernées.

Des limites à leur utilisation sont donc indispensables pour préserver les droits et libertés de chacun."

CNIL France

Compte tenu de l'augmentation des stocks et des flux de données personnelles dans les entreprises, **la solution Welcomr constitue une offre de rupture du contrôle d'accès pour des entreprises plus agiles, plus sûres et plus protectrices.**

POUR NOUS CONTACTER

contact@welcomr.com
www.welcomr.com

Blog

POSTFACE

Le RGPD est un cadre d'harmonisation du traitement des données personnelles au niveau européen et au rayonnement mondial avec lequel toutes les entreprises qui ont des intérêts économiques en Europe doivent se conformer.

Nous avons eu la chance de fonder Welcomr à une époque où la concertation juridique autour du RGPD battait son plein, traduisant l'importance du sujet du respect de la vie privée pour les citoyens européens.

Nous nous sommes donc employés à concevoir le premier système de gestion des accès éthique et responsable en matière d'accès aux données.

Par ailleurs, toutes les organisations doivent être préparées à une éventuelle violation de leurs données, et en particulier toutes celles qui gèrent de grandes quantités de données personnelles. En effet, l'économie digitale nécessite tant d'améliorer la connaissance et l'usage des nouvelles technologies et outils tels que l'Internet des objets, l'intelligence artificielle, et la 5G, que de maîtriser les capacités de stockage et le management sécurisé des données, dans un contexte où les volumes de données augmentent à grande vitesse.

Pour une conformité absolue au RGPD, il ne suffit pas que la gestion anticipe les notions d'autorisations d'accéder aux données. Il faut aussi que les pratiques de sécurité informatique protègent les données personnelles stockées dans la base de données de contrôle d'accès. A ce titre, la cybersécurité est chez Welcomr une préoccupation de tous les instants.

Welcomr se veut le premier contrôle d'accès éthique pour les entreprises qui ont l'ambition de rendre leurs bâtiments plus flexibles. Les équipes de Recherche & Développement de Welcomr s'emploient au quotidien à définir un nouvel Etat de l'Art pour la sécurité des données d'accès physiques.

Avec ce livre blanc, notre souhait était de vous partager notre conviction qu'en matière de protection des données personnelles, conception du logiciel de gestion des autorisations d'accès physiques et application des meilleures pratiques en matière de sécurité informatique vont de pair.

Alexis Gollain,
fondateur et Président de Welcomr