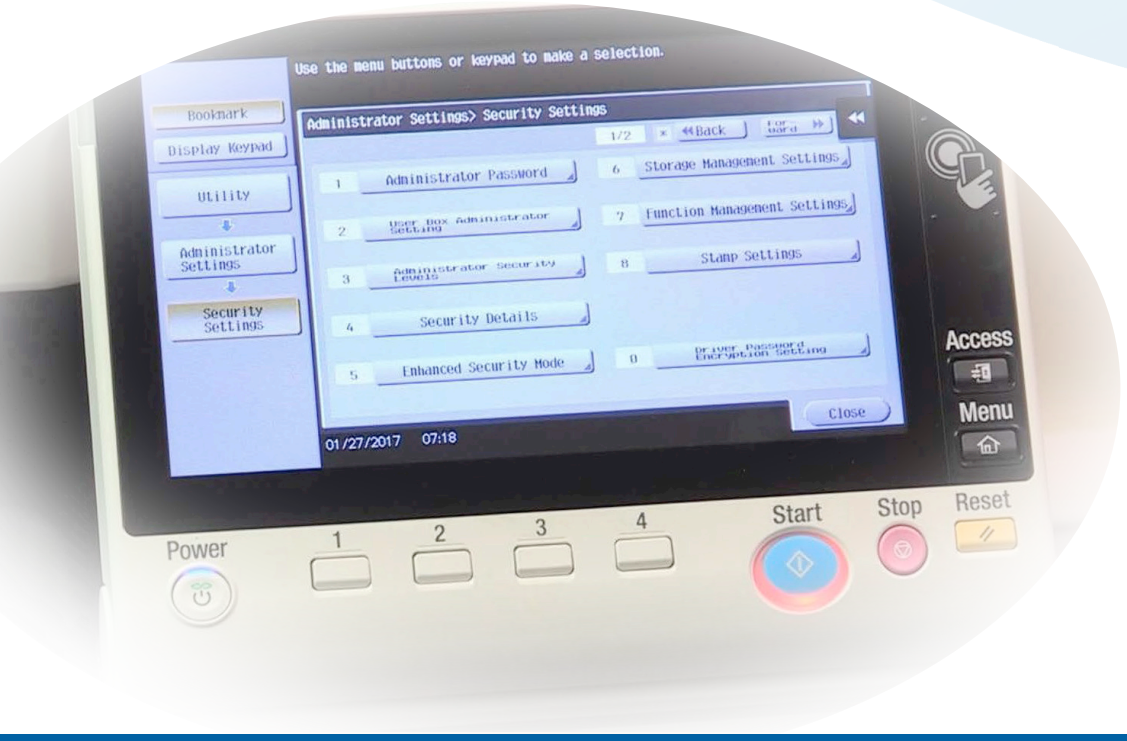
olivetti

Le RGPD

INTRODUCTION

LES PÉRIPHÉRIQUES MULTIFONCTIONS (MFP), LES SOLUTIONS DE FLUX DOCUMENTAIRES ET LES IMPRIMANTES RÉPONDENT PAR BIEN DES ASPECTS AUX STRICTS CRITÈRES DE LA SÉCURITÉ DES DONNÉES. DANS CE DOCUMENT DE SYNTHÈSE, NOUS IDENTIFIERONS CERTAINS DE CES ASPECTS POUR AIDER LE LECTEUR À MENER SES PROPRES ÉVALUATIONS. DE PLUS AMPLES RENSEIGNEMENTS PEUVENT ÊTRE OBTENUS AUPRÈS DES PARTENAIRES DISTRIBUTEURS DE LA MARQUE OLIVETTI ET DE L'ÉQUIPE DE SUPPORT TECHNIQUE D'OLIVETTI EN FRANCE.

CONTENU



LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) REMPLACE LA DIRECTIVE SUR LA PROTECTION DES DONNÉES 95/46/EC. IL A ÉTÉ CONÇU POUR HARMONISER LES LOIS SUR LA PROTECTION DES DONNÉES EN EUROPE ET POUR PROTÉGER ET RENFORCER LA CONFIDENTIALITÉ DES DONNÉES DES CITOYENS

Qu'est-ce que le RGPD?

Le Règlement Général sur la Protection des Données (RGPD) est un texte de Loi européen qui entre en application le 25 mai 2018. Il a été publié par l'Union Européenne pour améliorer la protection des données personnelles à travers l'Europe (y compris au Royaume-Uni). Ses exigences excèdent les lois existantes concernant la protection des données dans chacun des pays membres de l'UE offrent un cadre unifié de nouveaux règlements communs.

Ces nouveaux règlements ont été conçus car les différentes lois en vigueur se sont révélées de plus en plus insuffisantes ou inadaptées au fil des ans. Ces règlements cherchent à rendre toutes les personnes ou organisations qui recueillent, manipulent, stockent ou gèrent les données personnelles, responsables de la protection de ces données et à rendre responsables de leurs actes celles qui ne parviendraient pas à se conformer à ces nouvelles réglementations.

Le RGPD en un clin d'œil

A PARTIR DE QUAND CETTE NOUVELLE REGLEMENTATION EST APPLIQUEE?

Le 25 Mai 2018

QUI EST EN CHARGE DE L'APPLIQUER EN FRANCE ?

La Commission Nationale de l'Informatique et des Libertés (CNIL).

QU'EST-CE QUI CHANGE ?

De nouveaux droits permettant aux personnes d'avoir accès à leurs informations détenues par les entreprises ; des règles données aux entreprises pour une meilleure gestion des données et un nouveau régime d'amendes.

DE LOURDES PENALITES

Le règlement comporte de lourdes pénalités pour ceux qui ne s'y conforment pas. Des amendes allant jusqu'à 20 millions € ou 4% du chiffre d'affaires global d'une entreprise (celui des deux le plus élevé) peuvent être appliquées, ce qui est bien-sûr dévastateur sur le plan financier, mais porte également préjudice à la réputation de l'entreprise.

"Nous vivons dans un monde où les cyberattaques font partie de la vie" - *Business Reporter - The Telegraph*

Pourquoi le RGPD est-il devenu nécessaire?

Actuellement, chaque État membre de l'UE a ses propres directives en termes de protection des données. En France, c'est la Loi « Informatique et Libertés » qui s'applique depuis 1978.

Le fait est que la plupart de ces directives nationales ne permettaient pas de prendre suffisamment en compte l'évolution des technologies, rendant un grand nombre de ces lois inapplicables. Par conséquent, le RGPD vise à réunir tous les Etats membres sous un seul règlement, conçu pour être « à l'épreuve du futur » afin de permettre les avancées technologiques et les nouvelles méthodes commerciales des entreprises européennes ou de celles qui utilise des données européennes.

Avec un nombre de cyberattaques en recrudescence, la protection des données est vitale pour les entreprises et les particuliers. À l'heure actuelle, il est très difficile pour les personnes de savoir qui détient leurs données et ce qu'il en est fait. Le RGPD est destiné à mettre fin à ces inquiétudes.

C'est à un rythme exponentiel que prolifèrent partout dans le monde le nombre de données personnelles et force est de constater qu'elles sont de plus en plus exploitées par des sociétés peu scrupuleuses, des escrocs ou des pirates informatiques. Les risques sont donc également en très fortes augmentations.

Les risques liés aux violations des données personnelles sont encore trop souvent envisagés après la conception d'un produit ou d'un service, entraînant de plus en plus de retours, d'inadaptabilités, de réparations impossibles ou inefficaces ainsi que des d'échecs commerciaux.

"Si vous avez construit des châteaux dans les nuages, votre travail n'est pas vain ; c'est là qu'ils doivent être. À présent, donnez-leurs des fondations."
Henry David Thoreau, Author (1817-1862)

Plus de droits pour les individus

Le RGPD crée de nouveaux droits pour les individus et renforce certains des droits qui actuellement existent dans la Loi Informatique et Libertés.

Le RGPD fournit les droits suivants aux individus:

1. **Le droit à être informé**
2. **Le droit à l'accès**
3. **Le droit à la rectification**
4. **Le droit à l'effacement**
5. **Le droit à la restriction de traitement**
6. **Le droit à la portabilité des données**
7. **Le droit à l'objection**
8. **Droits relatifs à la prise de décision automatisée et au profilage**

“Une entreprise aura une bonne sécurité si sa culture d’entreprise est exemplaire. Et cela ne dépend que d’une chose : l’exemple qui vient d’en haut”

William Malik, VP and Research AD for Information Security- Gartner

Quels sont les principes clés de la nouvelle réglementation?

À qui s’adresse le RGPD ?

Le RGPD s’applique au « r**esponsable de traitement** » des données et au **«sous-traitant»**. Le responsable de traitement est celui qui sait comment et pourquoi les données personnelles sont traitées et le sous-traitant agit sur demande et au nom du responsable de traitement.

Le RGPD impose des obligations juridiques spécifiques aux sous-traitants. Par exemple, les sous-traitants sont tenus de conserver les archives des données personnelles et des activités de traitement. Les sous-traitants auront significativement plus de responsabilité juridique s’ils devaient être responsables d’une violation. Ces obligations pour les sous-traitants sont une nouvelle exigence émanant du RGPD.

Cependant, un responsable de traitement n’est pas pour autant déchargé de ses obligations lorsqu’un de ses sous-traitants est impliqué - le RGPD impose de nouvelles obligations aux responsables de traitement sur leurs sous-traitants afin qu’il soit fait état de la conformité avec le RGPD dans les contrats qui les lient.

Le RGPD s’applique à toute entité manipulant des données personnelles concernant des Européens, qu’il s’agisse d’une entreprise ou d’une association, et ce même si cette entité se trouve à l’extérieur de l’Union Européenne.

À quelles données le RGPD s’applique-t-il?

Données personnelles
Comme le règlement actuel, le RGPD s’applique aux «données personnelles». Cependant, la définition du RGPD est “toute information relative à une personne physique identifiée ou identifiable” et indique clairement que même des informations telles qu’un identifiant en ligne, une adresse IP ou des informations de localisation peuvent être des données personnelles.

Dans le cadre du RGPD, il existe un large éventail d ‘«identifiants personnels» qui constituent des données personnelles, reflétant les évolutions des

“ Le mantra de tout bon ingénieur de sécurité est : “La sécurité n’est pas un produit, mais un processus”. C’est plus que de concevoir une cryptographie forte dans un système : il s’agit de concevoir l’ensemble du système de sorte que toutes les mesures de sécurité, y compris la cryptographie, fonctionnent ensemble.”

Bruce Schneier - cryptographe et spécialiste des questions de la vie privée

technologies et la manière dont les organisations recueillent des informations sur les personnes.

Pour la plupart des organisations, conserver des informations telles que dossiers RH, listes de clients ou de coordonnées devrait faire peu de différence si les informations qu’ils contiennent relèvent de l’ancienne règlementation, car elles relèvent également de la compétence du RGPD.

Le RGPD s’applique à la fois aux données personnelles automatisées et aux systèmes de classement manuel là où les données personnelles sont accessibles selon des critères spécifiques. Cela peut inclure des ensembles d’enregistrements manuels contenant des données personnelles qui sont classées par ordre chronologique.
Si les données personnelles ont été codées avec un pseudonyme ou un pseudonyme, elles peuvent tout de même tomber dans le cadre du RGPD, selon le niveau de difficulté d’attribution du surnom ou du pseudonyme à un individu particulier.

Données personnelles sensibles

Les données personnelles sensibles selon le RGPD sont appelées “catégories spéciales de données personnelles”. Elles comprennent : les données d’origines raciales ou ethniques, les opinions politiques, les convictions religieuses ou philosophiques, l’appartenance à un syndicat, les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l’orientation sexuelle d’une personne physique.

L’article 5(1) du RGPD exige que les données à caractère personnel soient :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d’une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l’intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n’est pas considéré, conformément à l’article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l’identification des personnes concernées pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l’intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l’article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d’origine accidentelle, à l’aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

Article 5(2) : Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Technologie et RGPD

Le RGPD se compose de 8 grands principes qui couvrent tous les aspects de la réglementation. Le septième principe est celui qui peut être lié à la technologie impliquée dans le traitement et la gestion des données. Il implique les imprimantes et les outils de gestion de documents. Il stipule que **“des mesures techniques et organisationnelles appropriées doivent être prises contre le traitement non autorisé ou illégal de données à caractère personnel et contre la perte accidentelle ou la destruction ou l’endommagement de données à caractère personnel”**.

En pratique, cela signifie que les entreprises et les individus doivent disposer d’une sécurité appropriée pour éviter que les données personnelles détenues soient accidentellement ou délibérément compromises. En particulier, les entreprises devront :

- **Concevoir et organiser leur sécurité** en fonction de la nature des données personnelles qu’ils détiennent et des dommages pouvant résulter d’une atteinte à la sécurité ;
- **Avoir clairement défini qui, dans leur organisation, est responsable** de la sécurité de l’information ;
- **S’assurer qu’elles ont la bonne sécurité physique et technique**, renforcée par des politiques et des procédures solides et par un personnel fiable et bien formé; et
- **Etre prêtes à répondre** à toute violation de la sécurité rapidement et efficacement.

La plus grosse erreur qu’un utilisateur de matériel informatique puisse faire est d’ignorer la sauvegarde de ses données. “ *CyberSmart.org*

Les avancées technologiques ont permis aux organisations de traiter de plus en plus de données personnelles et de partager l’information plus facilement. Cela présente des avantages évidents si elles collectent et partagent les données personnelles conformément aux principes de protection des données, mais cela entraîne également des risques de sécurité tout aussi évidents.

Plus il y a de bases de données mises en place et plus les informations échangées sont nombreuses, plus le risque est grand que ces informations soient perdues, corrompues ou mal utilisées.

Ces dernières années, des pertes notoires de grandes quantités de données personnelles ont attiré l’attention sur la question de la sécurité de l’information.

Ces incidents ont également montré clairement que la sécurité de l’information est une question d’intérêt public ainsi que de conformité technique. Si les données personnelles ne sont pas correctement sécurisées, cela peut nuire gravement à la réputation et à l’avenir d’une organisation et peut également compromettre la sécurité des individus.

"En créant une stratégie pour protéger chaque niveau de données de manière appropriée, les entreprises peuvent sécuriser adéquatement les données contre les menaces d'aujourd'hui".
Chuck Davis, Professeur et Senior Security Architect

Sécurité via les périphériques multifonctions et les solutions documentaires

Les appareils multifonctions (MFP) tels que les imprimantes et les scanners sont souvent négligés lorsqu'il s'agit de la sécurité des données. Ils sont connectés au réseau de l'entreprise et permettent un grand nombre d'opérations aux utilisateurs, telles que de scanner un document pour l'envoyer par email ou sur le Cloud. Ils peuvent également stocker un certain nombre de données personnelles, telles que des adresses e-mail et IP et peuvent également enregistrer des tâches dans leur mémoires sophistiquées pour permettre aux gens de les imprimer à un stade ultérieur.

Il existe de nombreuses solutions logicielles basées sur le Web qui relient les produits MFP à la numérisation de documents, permettant aux entreprises d'intégrer des flux de production papier, des courriels et des fax entrants aux systèmes de gestion de documents, bases de données, serveurs de fichiers d'entreprise et applications de gestion de contenu. Il s'agit d'une forme de capture de données qui, de par leur nature, sont sous la responsabilité des responsables de traitement et des sous-traitants (cf. Page 5). Cependant, dans le cas de certains produits, tels que ceux qui ne stockent pas de données dans leur propre mémoire (ils transfèrent les données vers un stockage déporté, qu'il s'agisse du Cloud ou d'autres périphériques de stockage numérique), ceux-ci ne contiennent pas d'informations après le traitement des données.

Que faire pour vérifier son niveau de conformité ?

De nombreux aspects sont à évaluer minutieusement pour prévenir d'éventuelles violations de votre sécurité. Tout d'abord, les autorités officielles conseillent d'utiliser une checklist et de procéder à une évaluation des risques liés aux activités de capture, de manipulation, de traitement et de stockage des données. D'autre part, il convient d'évaluer les risques liés à la façon dont les informations sont partagées et imprimées ainsi qu'à ce qui arrive aux documents imprimés et comment et où ils sont classés.
Il est également sage de mettre en place une stratégie et même un plan d'urgence pour le traitement d'un potentiel incident lié à la sécurité des données. Une fois qu'une stratégie est en place, il est possible de s'assurer que les imprimantes, MFP et solutions de gestion de documents ont été mis en place avec les derniers kits de sécurité, systèmes d'authentification et possibilités de cryptages.

"Our names thus circulate far beyond our control among others who do indeed make a gain."
- David Lyon The Electronic Eye: The Rise of Surveillance Society

“La sûreté et la sécurité n’arrivent pas par hasard, elles sont le résultat d’un consensus collectif et d’investissements publics.”
Nelson Mandela

De quelles façons nos produits sont-ils compatibles avec le RGPD?

Selon le Règlement Général pour la Protection des Données, les imprimantes et les copieurs multifonctions (MFP) doivent être traités comme tout périphérique informatique puisqu’ils sont connectés au réseau, dotés de processeurs et utilisent pour la plupart des unités de stockage.

Les imprimantes, MFP et logiciels de gestion documentaire commercialisés par Olivetti ont été développés pour protéger les utilisateurs des accès non autorisés et des fuites d’informations, que ce soit à travers un réseau, via des périphériques mobiles, par la copie, par l’interférence ou la suppression d’informations dues à une défaillance de l’équipement, mais aussi par la perte ou par les dommages accidentels causés par un utilisateur ou enfin par un accès aux registres des travaux des périphériques d’impression (listes des tâches).

Nos copieurs multifonctions (MFP) les plus récents sont en conformité avec les standards de la norme Common Criteria (ISO/IEC 15408) ainsi qu’avec les normes de sécurité de l’IEEE 2600.1, soit en équipement de sécurité standard ou bien en options selon les matériels.
Comme il s’agit d’un sujet très vaste, nous ne couvrirons ici que quelques-uns des aspects fondamentaux de la façon dont les critères de sécurité de nos machines sont en phase avec le RGPD. Pour plus de détails, merci de contacter votre référent technique Olivetti.

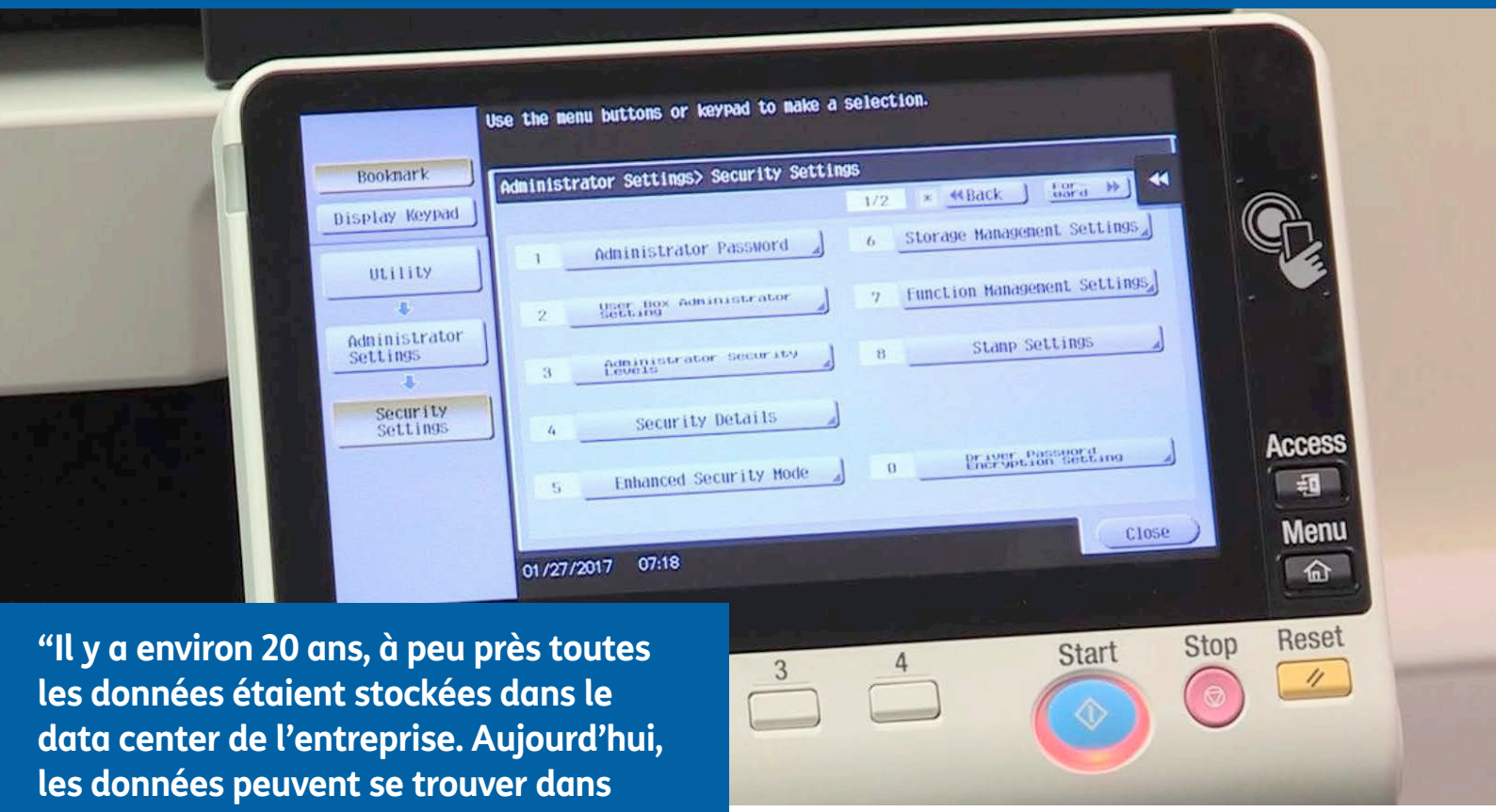
1. Sécurité lors du traitement des images et de leurs sorties

Lorsque des données sont numérisées via le scanner du MFP, elles sont traitées, compressées et écrites sur la mémoire du MFP. Pour imprimer ces données, elles sont décompressées et envoyées à l’imprimante, où elles sont imprimées sur du papier. Une fois l’impression terminée, les données compressées sont supprimées de la mémoire et les données images dans la mémoire sont écrasées page par page, de sorte qu’elles ne peuvent être réimprimées ou transférées.

Il est possible que les données de travail soient stockées sur le disque dur (HDD), sous la forme de données compressées uniques, mais même si ces données internes pouvaient être lues, leur analyse serait virtuellement impossible. De plus, sur la plupart des MFP Olivetti, le disque dur lui-même peut être crypté en standard. Il est également possible de verrouiller le disque dur par un mot de passe qui permet d’en empêcher les accès non autorisés.

En utilisant la fonction d’impression sécurisée, un travail d’impression peut être enregistré temporairement dans la mémoire du MFP, de façon à ce que l’utilisateur puisse l’imprimer plus tard, mais seulement après avoir entré un code PIN, un mot de passe ou en utilisant un des autres moyens d’authentification au MFP disponibles en standard ou en option selon les modèles (voir point suivant).

“Nous devons assumer la responsabilité de ces nouveaux pouvoirs et développer les éthiques correspondantes : éthique mondiale, éthique environnementale, éthique des générations futures, bioéthique, ainsi qu’une éthique de la technologie en général.” - *Hans Jonas - philosophe*



“Il y a environ 20 ans, à peu près toutes les données étaient stockées dans le data center de l’entreprise. Aujourd’hui, les données peuvent se trouver dans pleins d’endroits différents et parfois surprenants, tels que sur le Cloud public.”

Chris Evans - Computerweekly

2. Authentification utilisateur

Pour permettre une meilleure gestion de leur utilisation ou de leur accès, tous nos MFP peuvent être utilisés en mettant en place une authentification des utilisateurs préalable à toute utilisation. Il est alors possible de définir des règles d’autorisations (profils) pour des utilisateurs ou des groupes d’utilisateurs. Ces règles peuvent par exemple permettre un accès restreint à certaines fonctions importantes telles que le fax, la numérisation vers des e-mails (scan to email), l’accès aux données du disque dur, etc. Il est également possible de définir des quotas pour certains types de travaux. Nous pouvons vous proposer de nombreuses méthodes d’authentification possibles à nos périphériques d’impression : à partir d’un mot de passe personnel, PIN, carte d’authentification (badge), biométrie (analyse du réseau veineux d’un doigt) ou via un périphérique mobile via protocole NFC.

3. Protection des données sur le disque dur

Comme mentionné précédemment, les données résidant sur les disques durs des MFP Olivetti peuvent être écrasées afin de les en supprimer. Ceci est fait en réécrivant des couches de chiffres aléatoires. De plus, le disque dur peut être verrouillé, et rendu seulement accessible avec un mot de passe. Par conséquent, même si le disque dur est retiré de la machine et connecté à un PC, il ne pourra être consulté. Toutes les données sur le disque dur peuvent être cryptées avec le standard AES et par un module de cryptage intégré (OpenSSL / MES), de façon à ne pouvoir être lues ou décryptées sans leur clé de chiffrement.

L’activité du MFP est enregistrée dans un journal (liste des tâches). Celui-ci peut tracer tout accès non autorisé, mais il reste un simple outil de reporting et ne peut permettre l’accès, l’impression, le transfert ou la récupération des tâches ou des données précédentes.

4. Chiffrement des fichiers PDF

Les données numérisées sur le MFP et enregistrées au format PDF peuvent être chiffrées avec une clé commune ou un code. Pour ouvrir ces fichier PDF cryptés en utilisant Adobe Acrobat, il faudra entrer la clé commune ou le code.

5. Protection des données de courriers électroniques

Lorsqu’un utilisateur envoie un e-mail via le MFP Olivetti, il peut s’enregistrer dans le carnet d’adresses du destinataire en utilisant un code pour crypter son e-mail. Ainsi, le destinataire utilisera sa propre clé privée ou code pour déchiffrer l’e-mail qu’il reçoit sur leur PC. Cela permet de sécuriser l’envoi et la réception puisque l’email ne pourra ainsi pas être intercepté par d’autres personnes. L’expéditeur peut également ajouter une signature à son e-mail avec la clé du MFP, que le destinataire devra vérifier avec

“Agissez pour que les effets de vos actions soient compatibles avec la permanence de la vie humaine. “

Hans Jonas - philosophe

le certificat du MFP en utilisant une puce TPM. Cela permet au destinataire d’être assuré que l’email n’a pas été intercepté.

6. Scan to Me, Scan to Home et Scan to SMB

Un utilisateur peut s’envoyer à lui-même des données scannées à l’aide de l’authentification utilisateur du MFP Olivetti. Pour faciliter ces tâches, l’administrateur pourra paramétrer un bouton “Me” et/ou un bouton “Home” qui apparaîtront dans les adresses enregistrées de chaque utilisateur.

Si le bouton “Me” est sélectionné pour destination de la numérisation, le fichier numérisé sera envoyé par email à l’adresse de l’utilisateur authentifié (Scan to Me) et si “Home” a été sélectionné, il sera envoyé dans le dossier du PC enregistré à l’avance, permettant l’envoi rapide de fichiers en une seule touche (Scan to Home).

L’authentification SMB peut être restreinte aux adresses SMB autres que celles des utilisateurs en laissant vides les colonnes [ID utilisateur] et [mot de passe] de l’adresse SMB. Si un utilisateur connecté sélectionne sa propre adresse SMB dans le carnet d’adresses et appuie sur ‘envoyer’, alors le nom d’utilisateur et le mot de passe authentifiés sont utilisés sans changement.

En limitant et/ou en interdisant l’entrée directe de nouvelles adresses via les paramètres administrateur, il peut être décidé que seul l’administrateur est autorisé à gérer les destinations d’envoi, réduisant de fait les risques potentiels de mauvaises utilisations et l’envoi de données à des destinataires qui ne seraient pas autorisés.

7. Gestion des virus

Les contrôleurs d’impression de nos multifonctions couleur utilisent une plateforme Linux et sont de fait peu touchés par les virus qui visent la plupart du temps des systèmes d’exploitation Windows.

Dans la plupart des cas, les virus qui se trouvent sur des mémoires USB (clés) sont exécutés automatiquement et provoquent donc une infection du simple fait d’être connectées. Cependant, étant donné que nos MFP ne sont pas dotés d’un dispositif permettant l’ouverture des fichiers exécutables (dû à leur plateforme Linux), les virus qui pourraient se trouver sur une clé USB n’auront donc aucun effet.

Lors de la connexion d’une clé USB sur nos MFP, 3 possibilités se présentent à l’utilisateur :
(i) imprimer ses données stockées sur la clé
(ii) sauvegarder des données numérisées sur la clé
(iii) transférer des données stockées sur la clé USB vers le disque dur du MFP,
Ces trois possibilités doivent être activées par l’utilisateur, de sorte qu’elles ne s’auto exécutent pas et qu’il est facile d’en tracer l’auteur.

En outre, le chemin réseau et celui de l’interface USB sont séparés sur l’architecture système de nos MFP. Cela signifie donc que si on branche un PC connecté à Internet sur le MFP via le port USB, le MFP ne pourra être accédé depuis Internet au travers du PC.

www.olivetti.com

“Le terme utopie est souvent le moyen le plus pratique d’excuser ce que vous n’avez pas l’envie, la capacité ou le courage de faire. Un rêve ressemble à un rêve jusqu’à ce que vous commenciez à travailler dessus. Et c’est alors qu’il peut devenir quelque chose d’infiniment plus grand. “

Adriano Olivetti
Fondateur d’Olivetti