AUDIT RGPD

Réalisé pour :

Ecole d'Arts d'Avignon

500 chemin de Baigne Pieds

84 000 Avignon

Tél : 04 90 27 04 23

Avec Emilie Cosme et

Pascal Genty

Réalisé par :

Yann Riché

1965 chemin des Trespeaux 30100 Alès

Date – 09 juillet 2020 et 28/09/2021

LES CONTACTS BEA INFORMATIQUE

Toutes les demandes formelles concernant ce document doivent, être adressées à :

Le responsable commercial du compte

Votre premier contact chez BEA Informatique est :

Adresse postale :	*Guillaume Pujalte* BEA Informatique 1965 chemin de Trespeaux 30100 Alès
Téléphone :	+33 4 66 56 20 50
Mobile :	+33
Email :	g.pujalte@bea-informatique.fr

L'équipe dédiée

BEA Informatique met à votre disposition une équipe technique dédiée. Le rôle de cette équipe consiste en particulier à travailler en étroite relation avec vous, à la compréhension de vos exigences et des attentes de vos équipes.

Nom	Rôle	Téléphone	E-mail
Yann Riché	Consultant	06 17 17 17 26	y.riche@bea-informatique.fr
		00 00 00 00 00	.....@bea-informatique.fr

Confidentialité

BEA Informatique s'engage, dans le cadre de ses relations contractuelles, à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (RGPD).

TABLE DES MATIERES

1 INFORMATIONS SUR LE RGPD 5

1.1. TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL 5

1.1.1 Traitement de données papier et numériques 5

2.1.1 5

1.1.2 RGPD, loi Informatique et Liberté et usage personnel 5

1.1.3 Données soumises au RGPD 5

1.1.4 Principes du traitement de donnée 6

1.1.5 Licéité du traitement de données 6

1.1.6 Droits relatifs à la personne concernée 6

1.1.7 Droits d'opposition et d'effacement 7

1.2 MESURES A METTRE EN ŒUVRE 7

1.2.1 Protection des données à la conception 7

1.2.2 Sensibiliser les utilisateurs 7

1.2.3 Gestion des réclamations 8

1.2.4 Motifs de refus 8

1.2.5 Déclarer les violations de données 8

2. ETAT DES LIEUX DU PARC INFORMATIQUE 9

2.1 POSTES CLIENTS 9

2.2 ANTIVIRUS 9

2.3 SERVEUR 9

2.3.1 Salle informatique 9

2.3.2 Onduleur 9

2.3.3 Serveur physique 9

2.3.4 Serveur virtuel 10

2.3.5 Firewall 10

2.3.6 Messagerie 10

2.3.7 Sauvegardes et stockage 10

2.3.8 Droits d'accès 10

2.3.9 Accès distants 10

2.3.10 Autre(s) équipement(s) 11

3. ANALYSE DE RISQUE 12

3.1 ANALYSE DE RISQUE : DONNEES A CARACTERES PERSONNEL 12

3.2 ANALYSE DE RISQUE : TECHNIQUE 12

3.3 ANALYSE DE RISQUE : ORGANISATIONNELLE 13

4. PRECONISATIONS 14

4.1 PRECONISATIONS TECHNIQUES 14

4.2 PRECONISATIONS ORGANISATIONNELLES 14

4.2.1 Sensibilisation aux utilisateurs 14

4.2.2 Gestion des droits d'accès au serveur 14

4.2.3 Traitements des données sensibles 14

4.2.4 Sécurisation des documents « papiers » 15

4.2.5 Gestion des documents « doublons » 15

4.2.6 Politiques de droit à l'oubli ou à la rectification 15

4.2.7 Politique d'archivage et de destruction 15

4.2.8 Politique de détection : cyberdéfense 15

5. CAMPAGNE D'INFORMATION 16

5.1 CAMPAGNE D'INFORMATION PAR E-MAIL 16
5.2 CHARTE INFORMATIQUE ET CHARTE DE CONFIDENTIALITE 16

1 INFORMATIONS SUR LE RGPD

1.1. TRAITEMENTS DE DONNEES A CARACTERE PERSONNEL

1.1.1. RGPD, ou règlement général pour la protection des données est une réforme européenne, qui est en application depuis le 25 Mai 2018.
1.1.2. Il vise à renforcer la protection des données à caractères personnel. Pour cela, le RGPD va renforcer les principes de la loi Informatiques et Libertés, en donnant aux utilisateurs plus de droits et de maitrise quant aux données les concernant.
1.1.3. Les entreprises devront donc tout mettre en œuvre pour que les données des utilisateurs soient protégées : on parle de respect des règles de l'art et d'obligation de moyen.
1.1.4. Si ce n'est pas le cas, l'entreprise pourra être sanctionnée financièrement. Il s'agira d'une sanction de 4% de son chiffre d'affaire annuel, à hauteur de 20 Millions d'euros.
1.1.5. Pour assurer le respect du RGPD, la CNIL sera le principal pouvoir de contrôle. Elle pourra, comme elle le fait déjà, procéder à des vérifications dans les locaux des entreprises, en ligne, sur audition et sur pièces. Dans un premier temps, il s'agira de contrôles liés aux plaintes qu'elle aura reçu. Lors de contrôle, l'entreprise devra obligatoirement fournir son registre RGPD afin de prouver sa bonne foi.

2. La CNIL fait cependant une distinction, en ce qui concerne les contrôles :
3. Elle continuera à sanctionner pour ce qui concerne le non-respect des principes fondamentaux déjà établis (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données...)
4. Elle sera plus tolérante et aura un rôle d'accompagnateur en ce qui concerne le RGPD. Toutefois, l'entreprise devra prouver sa bonne foi, et démontrer qu'elle a déjà commencer à appliquer les principes du RGPD.

1.1.1 Traitement de données papier et numériques

Le RGPD impose la protection des données à caractère personnel, comme nous l'avons vu précédemment. Cependant, bien que souvent associées au monde du numérique, le RGPD concerne aussi tout traitement d'informations informatisés ou non.

Un fichier papier organisé selon un plan de classement, des formulaires papiers nominatifs, des dossiers de candidatures, etc… sont des données à caractère personnel soumises à un traitement.

2.1.1

1.1.2 RGPD, loi Informatique et Liberté et usage personnel

Le RGPD et la loi Informatique et Liberté ne s'appliquent bien évidemment pas à un usage EXCLUSIVEMENT personnel. Toute données telles qu'un répertoire personnel de contacts, des photos de vacances, des conversations mail privées, etc… ne sont pas soumises au RGPD.

1.1.3 Données soumises au RGPD

Comme nous avons pu le voir, des données permettant d'identifier une personne comme un fichier client, un carnet d'adresse ou une base de données peuvent être soumises au RGPD car nous parlons de traitement de données.

Plus généralement, toute donnée soumise à un traitement automatisé est aussi soumise au RGPD.

1.1.4 Principes du traitement de donnée

Pour respecter le RGPD et la loi informatique et libertés, plusieurs principes doivent être appliqués quant au traitement des données.

Les données doivent être traitées de manière licite, loyale, et transparente.

De plus, elles doivent être collectées à des finalités bien déterminées, explicites et légitimes. Ces données ne doivent en aucun cas être ultérieurement traitées dans des buts incompatibles avec les buts de départ. On parle de minimisation des données.

Par exemple, il est disproportionné de collecter des données telles que les orientations sexuelles et religieuses d'une personne pour créer une carte de fidélité dans une boutique de vente d'objets décoratifs.

Les données doivent aussi être conservées pendant une période nécessaire au regard des finalités pour lesquelles elles sont traitées.

1.1.5 Licéité du traitement de données

Le traitement des données doit être licite. Pour cela, il doit remplir au moins une des conditions suivantes :

La personne a consenti au traitement de ses données à caractère personnel pour une ou des finalités spécifiques.

- Le traitement est nécessaire à l'exécution d'un contrat auquel la personne est concernée.
- Le traitement est nécessaire au respect d'une obligation légale.
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée.
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

1.1.6 Droits relatifs à la personne concernée

Le responsable du traitement de données doit prendre des mesures appropriées pour fournir tout information de façon concise, transparente, accessible et compréhensible.

Ce même responsable doit pouvoir fournir les informations relatives aux finalités du traitement, les destinataires des données à caractère personnel, la durée de conservation si possible, l'identité et les coordonnées du responsable du traitement, et éventuellement les coordonnées du DPD.

1.1.7 Droits d'opposition et d'effacement

Toute personne concernée par un traitement de données à caractère personnel a le droit de s'opposer à tout moment, pour des raisons la regardant, à ce traitement de données.

De même, qu'elle a le droit d'obtenir du responsable du traitement de données l'effacement de ses données à caractère personnel dans les délais les plus courts. Le responsable a l'obligation d'effacer les données.

Enfin, comme précédemment, il existe un droit de rectification, si des données à caractère personnel s'avéraient inexactes.

1.2 MESURES A METTRE EN ŒUVRE

L'organisation des processus va impliquer plusieurs étapes dans la mise en conformité du RGPD.

1.2.1 Protection des données à la conception

La première étape, n'est pas applicable à toutes les infrastructures. En effet, elle concerne la prise en compte de la protection des données dès la conception d'un logiciel, application, SI… etc. De façon générale, elle concerne tout nouveau traitement de données.

Bien que cela soit applicable aux nouveaux traitements de données, il faut aussi appliquer les principes de protection des données à caractère personnel à toute données du SI. Il s'agira donc de minimiser la collecte des données, réguler la conservation des données, revoir les mentions d'informations, recueillir le consentement des personnes impliquées, assurer la confidentialité et la sécurité des données…

1.2.2 Sensibiliser les utilisateurs

Le second processus, sera de sensibiliser les utilisateurs et organiser la remontée d'informations. L'entreprise devra donc organiser un plan de formation et de communication pour ses collaborateurs.

Il est primordial pour l'entreprise de communiquer sur le RGPD et informer ses collaborateurs.

1.2.3 Gestion des réclamations

Le troisième processus concerne le droit à l'effacement, à l'oubli, et à la rectification. Il s'agira pour l'entreprise de savoir comment et qui gèrera les réclamations et demandes de personnes concernées. Il peut s'agir de traitements par voie postale ou voie électronique.

1.2.4 Motifs de refus

Dans certains cas, l'entreprise peut refuser de répondre aux demandes de droit d'accès :

- S'il s'agit de demandes abusives (comme vu précédemment)
- Si pour des raisons techniques, les données ne sont pas conservées
- Si la demande intervient après la durée légale de conservation

Attention : il est cependant **obligatoire** pour l'entreprise de répondre à la demande, même s'il s'agit d'une réponse négative.

1.2.5 Déclarer les violations de données

Enfin, le dernier processus concerne la violation des données. Pour l'entreprise, il s'agira de pouvoir détecter et notifier dans les 72 heures les autorités de protection des données dans le cas d'une attaque. Cette étape est assez complexe, car une attaque peut être découverte des semaines voir des mois après l'infiltration.

La CNIL a mis en production un télé service de notification, afin de simplifier les déclarations de violations, qui est disponible depuis Mai 2018.

La procédure relative à la violation notifiée pourra être clôturée si la CNIL constate que :

- La violation ne porte pas atteinte aux données à caractère personnel ou à la vie privée des individus.
- Les personnes concernées sont informées.
- Les règles de l'art ont été respectées en ce qui concerne les mesures techniques de sécurité.

La CNIL pourra imposer d'informer les personnes concernées si elle constate que :

- Les personnes n'ont pas été correctement informées.
- Les mesures techniques de protection mises en place préalablement à la violation ne sont pas appropriées.

2. ETAT DES LIEUX DU PARC INFORMATIQUE

2.1 POSTES CLIENTS

- Nombre de postes dans l'entreprise :
- Qui utilise ces postes ?
- Remarques supplémentaires :
-

LA Liste de l'équipement maintenu à jour par le responsable informatique, Pascal Genty, il gère par ailleurs les mots de passe des utilisateurs (attributions, réinitialisation) et gère la sécurité informatique dans son ensemble (Serveurs, postes, anitvirus, wifi…)

2.2 ANTIVIRUS

- Nom(s) de(s) antivirus utilisé(s) :
- Dernière(s) date(s) de mise à jour :

2.3 SERVEUR

2.3.1 Salle informatique

- Localisation de la salle informatique : La salle informatique est identifiée et climatisée. L'accès est restreint et limité au responsable informatique.
- Remarques supplémentaires : Local sous contrôle d'accès

2.3.2 Onduleur

L'onduleur permet une protection en cas de coupure de courant.

- Y a-t-il un onduleur dans l'entreprise ? Oui
- Remarques supplémentaires :

2.3.3 Serveur physique

- Photo :
- Description :

2.3.4 Serveur virtuel

- Schéma réseau (si donné par l'entreprise cliente)
- Explication du schéma réseau

L'EAA dispose d'un serveur pour l'administration et d'un serveur pour les élèves (salle informatique).

Le serveur Z est géré par des droits selon les fonctions du personnel.

2.3.5 Firewall

- Marque du firewall :
- Modèle :

2.3.6 Messagerie

- Boîte de messagerie utilisée :
- Présence d'un anti-spam ? oui

2.3.7 Sauvegardes et stockage

- Méthode de sauvegarde :NAS
- Lieu de stockage des données récoltées : Sur site
- Test de restauration :
- Remarques supplémentaires : Les deux outils principaux sont les logiciels de gestion de l'EPCI et celui de gestion des élèves (déploiement en cours 09-2021) à l'issue du déploiement du nouveau logiciel 'Ganesh », un test des sauvegardes et de restauration peut être envisagé pour l'ensemble des logiciels.

2.3.8 Droits d'accès

- Accès physiques : Pascal Genty à accès au serveur – Local sous clé
- Accès logiques : Chacun dispose d'un compte et d'un mot de passe personnalisé – Les accès aux répertoires sur le serveur sont gérés.

2.3.9 Accès distants

- Accès à distance possible avec ordinateur allumé – accès par le session du poste.

2.3.10 Autre(s) équipement(s)

- Exemples : vidéo surveillance, wifi

L'EAA dispose d'un wifi non sécurisé. En septembre 2021, une commande est passée par installer un réseau wifi permettant de tracer les navigations et de mieux contrôler les connexions.

Un contrôle d'accès est en place au sein des bâtiments pour le personnel avec des zonages spécifiques selon les bureaux / personnels.

3. ANALYSE DE RISQUE

L'analyse de risque se base sur l'estimation des risques sur une échelle à trois niveaux, ainsi on considère qu'un risque peut être :

- Faible
- Modéré
- Elevé

Le niveau de risque d'un élément permet d'estimer l'importance du fichier pour l'entreprise, mais aussi des éléments contenant des données à caractères personnel utilisés. L'emplacement de stockage des données sensibles permet de réduire le risque lié à la perte ou vol de ces données.

Cas de l'entreprise Ecole Supérieure d'Arts d'Avignon

3.1 ANALYSE DE RISQUE : DONNEES A CARACTERES PERSONNEL

L'organisation de l'information est structures autour du serveur de l'établissement et de logiciels clés,

Berger Levrault spécialisé pour la gestion des établissements publics pour la paye, les carrières de fonctionnaire et la gestion des fournisseurs et clients.

Ganesh pour la gestion des inscriptions et du suivi des élèves (en déploiement en 2021-2022

Le site et le serveur sont sécurisés et permettent d'avoir un risque faible de perte ou de corruption de données.

Berger Levrault, dispose d'une compliance RGPD, le 14 mai 2021, l'entreprise a subi une attaque de ransomware qui a été neutralisée. Les clients du logiciel en ont été informés.

Un second logiciel clé est en cours d'installation, Ganesh, pour assurer les inscriptions et le suivi des parcours des étudiants (notes, présences, dossiers).

3.2 ANALYSE DE RISQUE : TECHNIQUE

Le point sensible du système est le Wifi sur lequel il n'y pas de traçabilité des connexions. Ce risque est en cours de résolution

3.3 ANALYSE DE RISQUE : ORGANISATIONNELLE

Emilie Cosme, Déléguée à la protection des données, est opérationnelle et intervient en réunion pour cadrer les sujets de protection de données, création de fichiers, etc. La procédure d'archivage est à formaliser (archivage papier et informatique).

Il n'y a pas de charte informatique ni pour l'administration ni pour les élèves. Le point important est de prévoir des sensibilisations à destination des personnels.

4. PRECONISATIONS

Légende	Priorités
Préconisation très fortement recommandée, voire indispensable	
Préconisation importante et recommandée (à mettre en place dès que possible)	
Préconisation non indispensable mais recommandée	

4.1 PRECONISATIONS TECHNIQUES

Points à revoir	Améliorations possibles	Priorités
WIFI	Changer le Wifi et la gestion des connexions des logs	

4.2 PRECONISATIONS ORGANISATIONNELLES

4.2.1 Sensibilisation aux utilisateurs

Améliorations possibles/conseils/exemples	Priorités
Prévoir des ateliers de sensibilisation au cyber « risques » et à la gestion des mots de passe à destination du personnel, des enseignants et des élèves.	

4.2.2 Gestion des droits d'accès au serveur

Améliorations possibles/conseils/exemples	Priorités

4.2.3 Traitements des données sensibles

Améliorations possibles/conseils/exemples	Priorités
Charte informatique permet de faire un rappel sur l'utilisation des données	
Organisation du télétravail sur la gestion des postes et accès au réseau à distance – comment sont stockées les données – procédure en cas d'accès non autorisé.	

4.2.4 Sécurisation des documents « papiers »

Améliorations possibles/conseils/exemples	Priorités

4.2.5 Gestion des documents « doublons »

Améliorations possibles/conseils/exemples	Priorités
Gestion des doublons à voir avec la procédure archivage (permet de gagner de la place sur les serveurs)	

4.2.6 Politiques de droit à l'oubli ou à la rectification

Améliorations possibles/conseils/exemples	Priorités
Procédures existantes qui peuvent être formalisées (pour Facebook et pour les dossiers en identifiant un mail de contact pour formaliser les demandes).	

4.2.7 Politique d'archivage et de destruction

Améliorations possibles/conseils/exemples	Priorités
Procédure d'archivage à formaliser (règles de l'administration + lieux de stockage)	

4.2.8 Politique de détection : cyberdéfense

Améliorations possibles/conseils/exemples	Priorités

5. CAMPAGNE D'INFORMATION

Afin de respecter les nouvelles normes liées au RGPD, plusieurs campagnes d'informations devront être faite par l'entreprise traitant des données à caractère personnel.

5.1 CAMPAGNE D'INFORMATION PAR E-MAIL

Il s'agira, d'informer toute personne qui aura par le passé été soumise à une collecte de données à caractère personnel. Les campagnes peuvent se faire par mail.

Un exemple de mail d'information sera fourni par BEA Informatique.

5.2 CHARTE INFORMATIQUE ET CHARTE DE CONFIDENTIALITE

La charte de confidentialité devra être transmise aux utilisateurs (salariés, fournisseurs/sous-traitants, clients), dans le but de les informer des mises à jour liées au RGPD.

Pour tout nouvel utilisateur, la charte de confidentialité devra être présentée. Elle pourra être diffusée par mail, courrier postal ou par papier lors de la signature d'un contrat ou d'une récolte d'information.

La charte informatique pourra être révisée, afin de mentionner que les données sont collectées car légitimes.

Cette charte de confidentialité est fournie par BEA Informatique.