eurécia	**ETUDE IMPACT TRAITEMENT LOGICIEL SIRH EURECIA**	N° : RGPD/PIA/002/v1.1 Version : **1**
Date de validité : 28/05/2018	Destinataires : Clients Eurécia, Salariés Eurécia	

Informations du PIA

Nom du PIA
Logiciel SIRH Eurécia 1.1

Nom de l'auteur
Vincent Galvagnon

Nom de l'évaluateur
Jean-Luc Salasca

Nom du validateur
Jean-Luc Salasca

Date de création
05/10/2018

Nom du DPD
Jean-Luc SALASCA

Opinion du DPD
Le traitement Logiciel SIRH Eurécia est conforme au RGPD. Les mesures de sécurité sont adaptées à la gravité et à la vraissemblance des risques identifiés.

Recherche de l'avis des personnes concernées
L'avis des personnes concernées a été demandé.

Noms des personnes concernées
Directeur Général, Directeur R&D

Statuts des personnes concernées
Le traitement pourrait être mis en oeuvre.

Opinions des personnes concernées
Le traitement Logiciel SIRH Eurécia est conforme au RGPD. Les mesures de sécurité sont adaptées à la gravité et à la vraissemblance des risques identifiés.

Contexte

Vue d'ensemble

Quel est le traitement qui fait l'objet de l'étude ?
Le PIA porte sur **le Logiciel SIRH Eurécia pour la gestion des ressources humaines.**

Composée de 10 modules le Logiciel permet à la société cliente d'Eurécia d'exploiter les fonctionnalités de gestion des ressources humaines pour ses salariés : Portail RH, Congés & Absences, Notes de frais, Temps et Activités, Planning,

Compétences, Entretiens, Formations, Recrutement, Bien Etre.

Le logiciel SIRH Eurécia est accessible en mode SAAS (Software As A Service).

Quelles sont les responsabilités liées au traitement ?

Le **Client Eurécia** utilisateur du Logiciel SIRH Eurécia est **Responsable de Traitement** dont la finalité est la gestion RH de ses salariés et traite à ce titre les données personnelles afférentes de ses salariés.

Eurécia fournisseur du Logiciel SIRH **est Sous-Traitant** amené à traiter, héberger, accéder, sauvegarder, restituer des données personnelles pour le compte du Client.

Quels sont les référentiels applicables ?

Les référenciels applicables n'étant pas disponibles, cette rubrique ne peut pas être renseignée.
Évaluation : Acceptable

Données, processus et supports

Quelles sont les données traitées ?

Données à Caractère Personnel traitées par le Logiciel SIRH Eurécia

Portail RH/Données Générales Modules : Civilité, Email, Nom, Prénom, Photo, Numéro de sécurité sociale, Numéro de téléphone professionnel, Adresse personnelle, Date de naissance, Nationalité, Situation familiale, Type de contrat de travail, Horaire de travail, RIB / IBAN, N° Carte bancaire, Numéro de téléphone personnel, Email personnel, Copie carte grise véhicule personnel + infos contenues sur carte grise , Contrat de travail (CDD/CDI), Statut professionnel (cadre / non cadre), Coefficient, Diplômes (copie numérique), Permis et habilitations (copie numérique), Justificatifs d'adresse (copie numérique), Carte de séjour (copie numérique), Contrat de travail (copie numérique), Date de naissance et âge des enfants, Salaire annuel brut, Salaire mensuel brut, Salaire journalier brut, Mode de paiement, Nom de la mutuelle, Formule de la mutuelle, Attestation sécurité sociale (copie numérique), Moyen de transport , personnel (dont détails), Manager, Matricule, Date embauche, Motif entrée, Motif départ, Type de contrat de travail et données afférentes (période essai, horaires,...), Statut professionnel, Ancienneté, Qualification et coeff, Eléments de rémunération complémentaire (TR, ...), Mutuelle + formule mutuelle (volet personnel), Fiche aptitude médicale au travail (+ données afférentes : dates de visites,....), Comptes LinkedIn, Viadeo, Twitter, Facebook, Commentaires libres, Champs dont on peut changer l'intitulé : libres, Mot de passe, Adresse IP utilisateur.

Module Congés & Absences : Infos congés (dates, solde, type absence, ...), Justificatifs de congés standard, Congés maladie salarié (justificatif d'arrêt de travail), Dècès d'un proche (justificatif d'arrêt de travail), Accident du travail, Congé parental, Congés enfant malade (justificatif d'arrêt de travail), Maternité/Paternité, Autres champs libres, Tickets restaurant.

Module Notes de Frais : Dates de déplacements professionnels, Justificatifs de frais professionnel, Informations indirectes sur les déplacements professionnels (trajets, horaires sur détails billets/factures), Informations indirectes sur les préférences alimentaires (détails factures restaurants).

Module Temps et Activités : Feuilles de temps traçant l'activité professionnelle (horaires,.....).

Module Planning : Planning prévisionnel de l'activité professionnelle (horaires,.....).

Module Compétences : Compétences professionnelles.

Module Entretiens : Entretien annuel (copie numérique).

Module Formation : Formations suivies, Projets de formation, Avis sur les formations reçues.

Module Recrutement : Nom candidat, Prénom candidat, Civilité, date de naissance, Email, Téléphone, Adresse, Expérience, CV candidat, Compte rendu entretien embauche, Nom, Prénom, Date de candidature, Poste recherché, Prétentions, Adéquation, Etat de la candidature, CV, Compte rendu entretien embauche.

Module Bien-Etre : Humeur, Feedbacks (commentaires).

Destinataires des Données :

- Client Eurécia : DG, DAF, DRH, Administrateurs du Logiciel SIRH Eurécia
- Eurécia : Editeur du Logiciel SIRH
- Sous-traitants Eurécia : FullSave, OVH (Hébergeurs); ITRUST (Expert Sécurité Informatique)

Comment le cycle de vie des données se déroule-t-il (description fonctionnelle) ?

1-Gestion des habilitations par le Client Eurécia : le client Eurécia définit les habilitations de chaque utilisateur du Logiciel SIRH selon un système hiérarchisé de règles de gestion spécifiques. Les principales catégories d'utilisateurs sont Administrateurs, Managers, Utilisateurs standards. Chaque utilisateur a un profil lui donnant accès à plus ou moins d'informations en fonction de ses droits.

2 - Création d'un compte Utilisateur standard par l'Administrateur ou le Manager du Client Eurécia.

3- Saisie des données personnelles générales liées à l'utilisateur par l'Administrateur ou le Manager (Module Portail RH ou données générales des 9 autres modules du Logiciel).

4- Saisie des données personnelles spécifiques aux modules souscrits par le Client Eurécia par l'utilisateur salarié du client Eurécia et/ou l'Administrateur ou le Manager du Client Eurécia et/ou tout autre utilisateur habilité.

5- Sockage et traitement des données dans le Logiciel SIRH Eurécia hébergée sur un serveur : stockage, validations, calculs, analyses, aggrégations, restitutions à partir des données saisies.

6- Consultation des données saisies dans le Logiciel ou produites par le Logiciel par l'utilisateur salarié, l'Administrateur ou le Manager et/ou tout autre utilisateur habilité

7- Relais d'information vers des applications tierces : applications de gestion de la paie, applications comptables, ERP,...

Quels sont les supports des données ?

1 - Création d'un compte utilisateur : serveurs cloud Fullsave, serveurs cloud OVH, internet, wifi, PC, smartphone

2- Saisie des données personnelles générales : serveurs cloud Fullsave, internet, wifi, PC, smartphone

3- Saisie des données personnelles spécifiques : serveurs cloud Fullsave, serveurs cloud OVH, internet, wifi, PC, smartphone

4- Sockage et traitement des données : serveurs cloud Fullsave, serveurs cloud OVH,

5- Consultation des données : serveurs cloud Fullsave, serveurs cloud OVH, internet, wifi, PC, smartphone

6- Relais d'information vers des applications tierces : serveurs cloud Fullsave, serveurs cloud OVH, internet, wifi, PC, smartphone

Évaluation : Acceptable

Principes fondamentaux

Proportionnalité et nécessité

Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

Les finalités du traitement des données collectées sont :

- **Déterminées** : les traitements effectués sont parfaitement déterninées pour le salarié du Client Eurécia qui est partie prenante du processus de gestion RH de son employeur.
- **Explicites** : les traitements effectués sont parfaitement explicites pour le salarié du Client Eurécia qui est partie prenante du processus de gestion RH de son employeur.
- **Légitimes** : le traitement des données personnelles dans le cadre de la gestion RH de ses salariés par un employeur constitue un traitement légitime

Évaluation : Acceptable

Quel(s) est(sont) les fondement(s) qui rend(ent) votre traitement licite ?

Le **traitement** de données par le Client Eurécia est **fondé sur le droit du travail et le contrat de travail** entre le Client Eurécia et son salarié pour les modules autre que le Module Recrutement et le Module Bien-Etre.

Traitement des données par le Module Recrutement : ce traitement de données relatives aux candidats au recrutement est fondé sur un intérêt légitime du Client Eurécia dans le cadre d'une candidature volontaire du candidat au recrutement.

Traitement des données relatives au Module Bien-Etre : ce traitement des données relatives à l'humeur des salariés est réalisé dans un intérêt légitime du Client Eurécia d'amélioration du Bien-Etre au travail de ses salariés. Le recueil des données est complètement facultatif pour le salarié. Enfin l'ensemble des données recueillies font l'objet d'une pseudonymisation.
Évaluation : Acceptable

Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ?

Toutes les données collectées sont strictement nécessaires pour couvrir l'intégralité des processus de gestion du personnel du Client Eurécia sur le périmètre des modules souscrits.
Évaluation : Acceptable

Les données sont-elles exactes et tenues à jour ?

Les salariés utilisateurs du Logiciel SIRH Eurécia ont un accès direct à leurs données personnelles à travers le Logiciel SIRH EURECIA et peuvent par conséquent en vérifier l'exactitude et les actualiser à tout moment.
Évaluation : Acceptable

Quelle est la durée de conservation des données ?

Pendant la période contractuelle entre son Client Eurécia et Eurécia :

Le Logiciel SIRH EURECIA offre la **fonctionnalité de suppression des données personnelles à tout moment par le Client Eurécia.**

En principe, dans le cadre des données relatives aux salariés, ces données pourront être conservées le temps de la période d'emploi de la personne concernée (sauf dispositions législatives ou réglementaires contraires; délais de prescription tel que prévus à l'article L1471-1 du Code du travail délais légaux de conservation...)

Cette fonctionnalité est activée par le Client Eurécia.

A tout moment pendant le temps du Contrat le Client peut demander à Eurécia d'opérer une réversibilité consistant en la remise par EURECIA des données hébergées du Client dans un espace de type Ftp où le Client pourra télécharger les données hébergées.

Au terme de la période contractuelle entre son Client et Eurécia :

Aux termes du Contrat, le Client peut demander à Eurécia d'opérer une réversibilité consistant en la remise par EURECIA des

données hébergées du Client dans un espace de type Ftp où le Client pourra télécharger les données hébergées.

Le Client peut demander cette réversibilité durant le temps du Contrat et au plus tard huit jours après son terme, quelle qu'en soit la cause, et l'accès aux données étant réservées au Client pendant une durée de cinq jours ouvrés, **toutes données hébergées du Client étant détruites au-delà de ces délais.**

Évaluation : Acceptable

Mesures protectrices des droits

Comment les personnes concernées sont-elles informées à propos du traitement ?

Le salarié utilisateur du Logiciel SIRH Eurécia ou le candidat au recrutement sont parfaitement informés des traitement de leurs données personnelles car :

- ils sont partie prenante du processus de gestion RH
- ils sont accès directement et à tout instant à leurs données personnelles
- ils sont informés par leur employeur, Client Eurécia et Responsable de Traitement

Évaluation : Acceptable

Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Compte tenu des motifs de liciété des traitements opérés par le Logiciel SIRH Eurécia, le recueil du consentement des personnes concernées n'est pas nécéssaire.

Concernant le module Bien-Etre : le recueuil des données étant complètement facultatif pour le salarié qui dispose de la possibilité de ne pas répondre, la soumission d'informations par le salarié vaut consentement.
Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Pendant son contrat de travail, **chaque salarié utilisateur a directement et à tout instant accès à ses données personnelles**. **Il peut également faire appel à son administrateur pour obtenir un export de type excel de l'ensemble de ses données.** Ces demandes sont soumises aux modalités définies par le Client, Responsable de traitement.

Après la rupture de son contrat de travail, chaque salarié peut exercer son droit d'accès à ses données personnelles selon les modalités prévues par le Client, Responsable de Traitement.

Le droit à la portabilité des données personnelles traitées par Le Logiciel SIRH Eurécia, **ne s'applique pas** pendant la durée de vie du contrat de travail, le salarié utilisateur étant sousmis à l'utilisation obligatoire de l'application de gestion RH choisie par son employeur.

Après la rupture du contrat de travail, la portabilité des données ne s'applique pas non plus les données personnelles étant strictement liées au contrat de travail.
Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de rectification et droit à l'effacement (droit à l'oubli) ?

Pendant son contrat de travail, chaque salarié utilisateur a directement et à tout instant accès à ses données personnelles et peut donc exercer son droit de rectification soit directement, soit par demande auprès de son administrateur selon les modalités définies par le Client, Responsable de traitement.

Pendant son conrat de travail le salarié ne peut exercer son droit à l'effacement étant soumis aux règles du droit du travail.

Après la rupture de son contrat de travail, chaque salarié peut exercer son droit à rectification sur demande à son ex-employeur selon les modalités définies par le Client, Responsable de traitement.

Après rupture du contrat de travail, le salarié peut exercer son droit à l'effacement après épuisement des délais règlementaires de conservation des données personnelles, sur demande à son ex-employeur selon les modalités définies par le Client, Responsable de Traitement.
Évaluation : Acceptable

Comment les personnes concernées peuvent-elles exercer leurs droit de limitation et droit d'opposition ?

Le droit de limitation et le droit d'opposition sur les données personnelles traitées par le Logiciel SIRH Eurécia, ne s'applique pas, les données traitées étant strictement nécessaires à la gestion RH des salariés et le salarié utilisateur étant sousmis aux règles du droit du travail liées à son employeur Client Eurécia ou a une démarche volontaire de demande d'emploi.
Évaluation : Acceptable

Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Les obligations de respect du RGPD ont été contractualisées avec Fullsave et OVH sous-traitants Hébergement et Itrust (expert sécurité).
Évaluation : Acceptable

En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Les données personnelles traitées par le logiciel SIRH Eurécia ne sont pas transférées en dehors de l'Union Européenne.
Évaluation : Acceptable

Risques

Mesures existantes ou prévues

Chiffrement

Toutes les connexions, entre le PC ou le SmartPhone de l'utilisateur, et les le serveurs cloud du Logiciel SIRH Eurécia chez FullSave, **se font en SSL via le protocole HTTPS.**

En base de données de l'application Eurécia, **sont encryptées en AES/ECB/PKCS5PADDING :**

- Les **coordonnées bancaires** des salariés utilisateurs (RIB)
- Le **numéros de Carte Bancaire** des salariés utilisateurs

Évaluation : Acceptable

Contrôle des accès logiques

Tous les accès au Logiciel SIRH Eurécia et aux données personnelles sont soumis à une **connexion par identifiant et mot de passe complexe renouvellé régulièrement et masqué**.

Chaque utilisateur possède ses propres droits d'accès en fonction de son habilitation à accèder à certaines données.
Évaluation : Acceptable

Lutte contre les logiciels malveillants

Les serveurs hébergeant le Logiciel SIRH Eurécia sont exploités sous Linux (Debian) et sont peu sensibles aux virus.

L'usage de droit d'accès sur les fichiers limite l'impact des logiciels malveillants.

Les postes de travail de l'équipe R&D Eurécia qui sont sous windows sont protégés par l'**antivirus Bitdefender.**

Un **firewall physique Stormshield** protège le réseau local de l'entreprise.

Évaluation : Acceptable

Sécurisation de l'exploitation

Nos procédures d'exploitation récurrente sont automatisées (déploiement de l'application, redémarrage...).

Pour les actions exceptionnelles nos faisons appel à notre infogérant (Fullsave) et rédigeons les procédures dans des tickets / mail qui suivent une procédure de validation.

Les serveurs sont mis à jour régulièrement, les mise à jour de sécurités sont automatisées par notre infogérant Fullsave.

Les salles serveurs sont sécurisées et nos données sont redondées dans un second datacenter.

L'accès à nos locaux est sécurisé par badge et l'accès au local serveur est restreint par badge (voir détails dans volet Sécurité Physique)

Un AD (active directory) manage l'accès à notre réseau et nos ressources, il est administré par un infogéreur (Apixis).

Évaluation : Acceptable

Minimisation des données

Sont appliqués : restriction de l'accès aux données par filtrage et retrait en fonction des droits du profil utilisateur.
Évaluation : Acceptable

Sauvegarde des données

L'ensemble des données du Logiciel SIRH Eurécia est redondés dans un second datacenter. Ses données sont stockée sur des Netapp qui réalisent des sauvegardent quotidiennent sur une semaine.

Des sauvegardes supplémentaires sont réalisées pour l'ensemble de la base de données sur une période d'un mois et demi ainsi que pour chaque société cliente individuellement.

Ces sauvegardes sont jouées régulièrements sur des environnements de tests pour valider leur intégrité.

L'ensemble des données reste localisé dans les datacenters de notre hébergeur Fullsave.

Évaluation : Acceptable

Maintenance

Notre hébergeur Fullsave a la charge de maintenir nos serveurs et l'environnement réseau en état fonctionnel.

Seul notre hébergeur Fullsave possède les droits administrateur sur les serveurs.

Les équipements sont redondés (serveur, switch, firewall, loadbalancer, baie netapp).

Les postes de travail et notre réseau local sont maintenus par la société Apixis.

Évaluation : Acceptable

Contrat de sous-traitance

Nos Hébergeurs FullSave et OVH sont conformes au RGPD.

Les informations sur leurs systèmes de sécurité, reprises dans le présent PIA, sont régulièrement communiquées à Eurécia et font l'objet d'un suivi permanent par l'équipe Exploitation Eurécia.

Les serveurs Fullsave sont scannés automatiquement par les outils Ikare de la société Itrust, expert en sécurité informatique, pour détecter toute nouvelle vulnérabilité.

Évaluation : Acceptable

Sécurité physique

Le Data Center Fullsave hébergeant le Logiciel SIRH Eurécia est équipé des mesures de sécurité physique suivantes :

- Protection et surveillance 24h/24, 7j/7
- Accès 24h/24, 7j/7 par cartes magnétiques
- Alimentations électriques sécurisées et ondulées
- Détection et protection anti-incendie
- Climatisations redondées et supervisées
- Vidéo-surveillance
- Baies fermées propriété de la société FullSave

L'accès aux locaux de notre hébergeur Fullsave, est soumis 24h/24 à un double contrôle d'accès (badges + empreinte biométrique).

Ce contrôle d'accès s'applique aussi bien pour les accès extérieurs que pour les circulations internes.

L'accès à une zone n'est possible que pour les visiteurs préalablement enregistrés et autorisés.

Tout visiteur non enregistré doit être accompagné par une personne ayant accès.

Les baies d'hébergement sont fermées verrouillées par code.

La sécurité des locaux est supervisée par une alarme présente sur l'ensemble du bâtiment.

Toute alerte (intrusion ou incendie) est immédiatement transmise à l'équipe support 24h/24, 7j/7.

Évaluation : Acceptable

Traçabilité

La journalisation actuelle porte sur les évènements systèmes classiques. Les enregistrements sont conservés un an.

Il n'y a pas en l'état actuel de journalisation extérieure.
Évaluation : Acceptable

Sécurisation des matériels

Nos postes de travail sont dans un inventaire (Active Directory). Ils sont protégés par mot de passe.

Tout matériel exploité chez notre hébergeur, Fullsave, est enregistré dans son inventaire.

Pour pallier à une défaillance matérielle, FullSave veille à conserver du matériel redondant, ou s'appuie sur des prestataires assurant une livraison dans des délais brefs.

Les plateformes sont cloisonnées : utilisation d'hyperviseurs, de volumes de stockage, de contextes de configuration dédiés à un client.

Évaluation : Acceptable

Eloignement des sources de risques

Chez notre hébergeur Fullsave, les consignes de sécurité sont strictes et communiquées à tous les intervenants (sous-traitants FullSave, Clients et leurs intervenants). Par exemple :

- le matériel doit être déballé à l'extérieur des zones techniques, interdiction d'introduire des cartons ou emballages plastiques

- la nourriture, les animaux sont interdits

Évaluation : Acceptable

Protection contre les sources de risques non humaines

Chez notre hébergeur Fullsave, il y a une redondance complète des groupes froids maintenant les serveurs à une température constante quelques soient les températures extérieures.

Double détection et protection incendie par brouillard d'eau par zone.

Le Datacenter Fullsave est localisé en zone non sismique, non inondable, et hors zone de risques industriels.

Évaluation : Acceptable

Organisation de la politique de protection de la vie privée

Eurécia a nommé **DPO pilote de la mise en conformité RGPD** et travaillant en étroite relation avec tous les services Eurécia.

Eurécia est accompagnée par le cabinet d'avocat spécialisé ITEANU.

Tous les collaborateurs Eurécia ont suivi une formation interne sur enjeux relatifs à la protection des données personnelles et le RGPD.
Évaluation : Acceptable

Gestion des personnels

Formation interne des nouveaux arrivants aux enjeux relatifs à la protection des données personnelles.

Suppression immédiate de tous les accès au Logiciel SIRH Eurécia et au réseau Eurécia pour les collaborateurs quittant Eurécia dans le cadre d'une procédure formalisée de gestion des arrivées et départs.
Évaluation : Acceptable

Sécurisation des canaux informatiques

Les serveurs sont équipés de firewall (pare-feux) locaux.

Un pare-feu physique de l'hébergeur Fullsave protège les serveurs d'Internet.

Un firewall physique StormShield protège le réseau local d'Eurécia.

Un AD (active directory) manage l'accès à notre réseau et nos ressources, il est administré par un infogéreur (Apixis).

Nos serveurs sont scannés automatiquement par les outils Ikare de la société Itrust, expert en sécurité informatique, pour détecter toute nouvelle vulnérabilité.

Des audits de sécurité en boite blanche sont réalisés périodiquement par les équipes d'Itrust.

Évaluation : Acceptable

Protection des sites web

Nos sites sont en HTTPS / TLS1.0 minimum et sont conformes aux normes actuelles.

Seule les hash des mots de passes sont stockés.

Nos cookies ne portent pas d'informations personnelles, ils sont à usage technique.

Nos serveurs sont scannés automatiquement par les outils Ikare d'Itrust pour détecter toute nouvelle vulnérabilité.

Des audits de sécurités en boite blanche sont réalisés périodiquement par les équipes d'Itrust.

Évaluation : Acceptable

Accès illégitime à des données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Usurpation d'identité bancaire, Usurpation d'identité (numéro NIR, carte de séjour,...), Divulgation non souhaitée d'informations sur la santé, Divulgation non souhaitée d'informations sur le motif de départ d'un salarié (licenciement,..), Divulgation non souhaitée d'informations sur les revenus, Publicité ciblée

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Vol de mot de passe

Quelles sources de risques pourraient-elles en être à l'origine ?

Source humaine interne Client (négligence du salarié lui-même), Source humaine interne Client (négligence de l'administrateur), Source humaine externe de type cyber attack

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, Chiffrement, Sécurisation des canaux informatiques

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Importante, L'usurpation d'identitié constitue le risque le plus important compte tenu de l'impact juridique (actions en justice potentielles) et économique potentiellement très important ainsi que sa durée qui peut s'étaler sur plusieurs années.

La divulgation d'informations non souhaitées sur la santé peu constituer un risque également important permettant à des individus mal intentionnés de cibler les personnnes vulnérables.

La divulgation d'informations non souhaitées sur la situation économique ou professionnelle (revenus, licenciement,...) présente avant tout un impact en terme d'image qui reste d'une gravité limitée.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, La vraisemblance du risque est estimée à négligeable compte tenu de l'ensemble des mesures de sécurité logiques, physiques et procédurales de l'application Eurécia.

Évaluation : Acceptable

Modification non désirées de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Erreur de calcul sur la rémunération, Erreur de calcul sur le solde de jours de congés, Elimination d'un candidat au recrutement, Non versement du salaire dans les délais

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Modification des coordonnées bancaires par un tiers malveillant, Modification de jours d'abence rémunérées ou non rémunérée, Modifications de données relatives à un candidat au recrutement, Modifications du nombre d'heures travaillées

Quelles sources de risques pourraient-elles en être à l'origine ?

Source humaine interne, Source humaine externe

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, Chiffrement

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Limitée, Délai de paiement de la rémunération rallongé.

Les erreurs de calcul sur la rémunération ou le solde de congés sont détectables.

L'élimination d'un candidat au recrutement reste un risque limité

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable,
La vigilance de l'utilisateur concernant son mot de passe pemet de limiter la vraisemblance à négligeable.

L'impact limité en terme de gravité et le caractère potentiellement détectable des impacts limite l'intérêt d'une modification intentionnelle des données.
Évaluation : Acceptable

Disparition de données

Quels pourraient être les principaux impacts sur les personnes concernées si le risque se produisait ?

Retard dans le versement de la paie, Retards administratifs dans le traitement des demandes du salarié

Quelles sont les principales menaces qui pourraient permettre la réalisation du risque ?

Panne matérielle sur le datacenter Fullsave, Erreur humaine au sein d'Eurécia ou de l'hébergeur, Cyber Attack contre l'hébergeur Fullsave

Quelles sources de risques pourraient-elles en être à l'origine ?

Source non humaine (incendie, météorite, inondation, explosion... sur le datacenter hébergeant les environnements d'Eurécia., Source humaine interne (erreur de manipulation), Source humaine externe (erreur de manipulation chez l'hébergeur), Source humaine externe malintentionnée

Quelles sont les mesures, parmi celles identifiées, qui contribuent à traiter le risque ?

Contrôle des accès logiques, Sauvegarde des données, Sécurisation des canaux informatiques

Comment estimez-vous la gravité du risque, notamment en fonction des impacts potentiels et des mesures prévues ?

Négligeable, Des mesures efficaces de sauvegarde sont mises en place, permettant de reprendre l'activité très rapidement sans perte de données.

Comment estimez-vous la vraisemblance du risque, notamment au regard des menaces, des sources de risques et des mesures prévues ?

Négligeable, La base de données est redondée sur un second datacenter, les baies de stockage sont redondées sur un second datacenter Fullsave et les machines virtuelles sont redondées chez un second hébergeur permettant une remise en service très rapide de l'application Eurécia.
Évaluation : Acceptable

Plan d'action

Principes fondamentaux

Aucun plan d'action enregistré.

Mesures existantes ou prévues

Chiffrement

undefined
Date prévue de mise en œuvre

Contrôle des accès logiques

undefined

Date prévue de mise en œuvre

Lutte contre les logiciels malveillants

undefined

Date prévue de mise en œuvre

Sécurisation de l'exploitation

undefined

Date prévue de mise en œuvre

Minimisation des données

undefined

Date prévue de mise en œuvre

Sauvegarde des données

Améliorer le PRA par l'ajout d'un site de secours actif supplémentaire chez un hébergeur différent

Date prévue de mise en œuvre 31/12/2018

Responsable de la mise en œuvre R&D EURECIA

Maintenance

undefined

Date prévue de mise en œuvre

Contrat de sous-traitance

undefined

Date prévue de mise en œuvre

Sécurité physique

undefined

Date prévue de mise en œuvre

Traçabilité

undefined

Date prévue de mise en œuvre

Sécurisation des matériels

undefined

Date prévue de mise en œuvre

Eloignement des sources de risques

undefined

Date prévue de mise en œuvre

Protection contre les sources de risques non humaines

undefined

Date prévue de mise en œuvre

Organisation de la politique de protection de la vie privée

undefined

Date prévue de mise en œuvre

Gestion des personnels

undefined

Date prévue de mise en œuvre

Sécurisation des canaux informatiques

undefined

Date prévue de mise en œuvre

Protection des sites web

undefined

Date prévue de mise en œuvre

Risques

Aucun plan d'action enregistré.