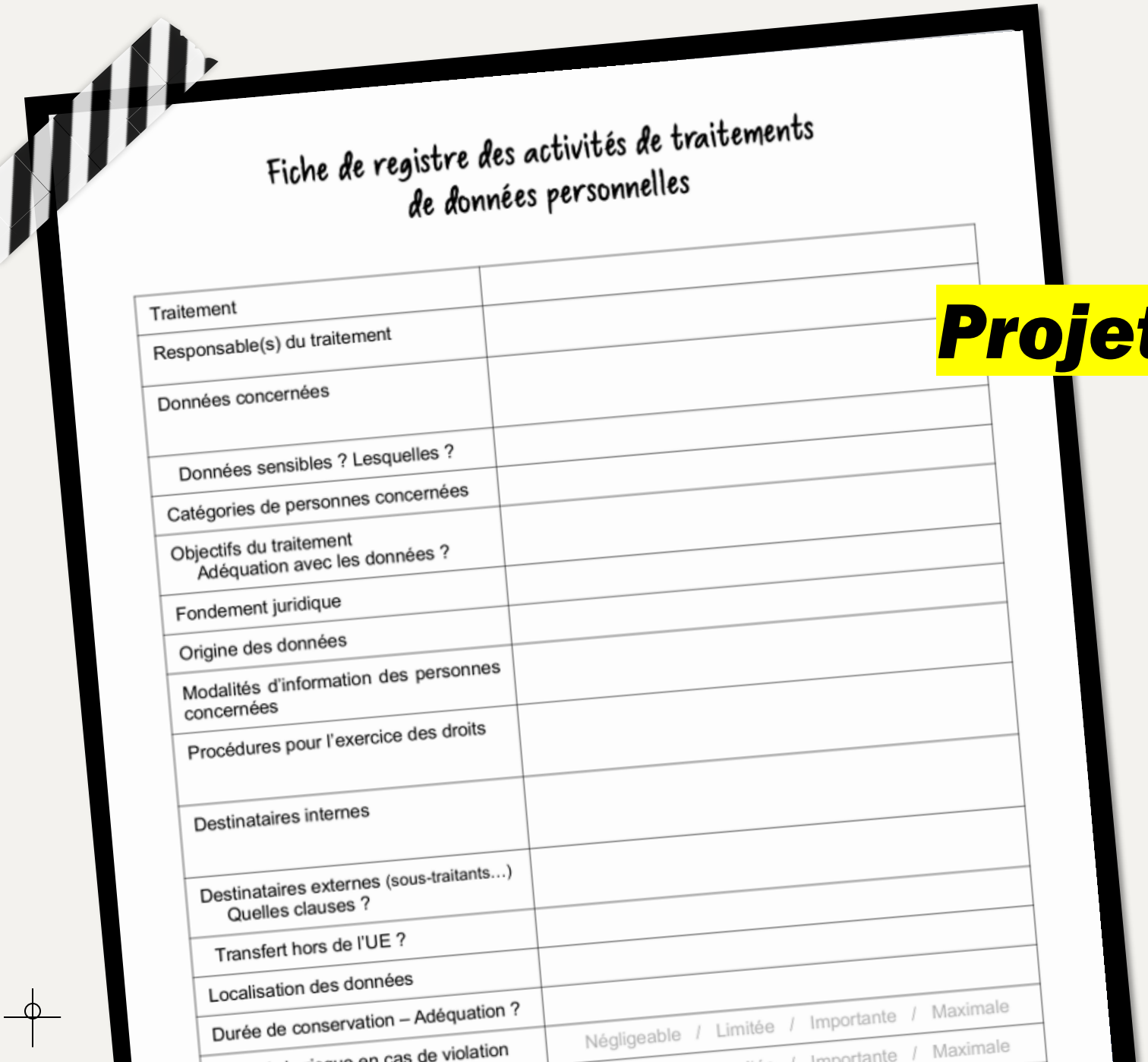

Projet RGPD

- Rose CHAUVIN
- Nathaël BENOIT
- Camille CARRACO
- Armand-Valentin GASSE

Contexte

- La société qui nous emploie est une entreprise industrielle, située en France, d’une centaine de salariés. La première urgence qui nous attend concerne le service « ressources humaines ». Ce service, qui n’a rien fait depuis l’entrée en application du RGPD, attend nos préconisations.
- Nous constatons à notre arrivée que les groupes de données suivantes sont traitées : Identification de l'employé ainsi que le suivi de la carrière et de la formation de l'employé.
- Nous devons alors déterminer très précisément et conseiller ce que doit faire l’entreprise pour être en conformité.

Les 5 principes du RGPD

- Tout d’abord le RGPD a comme principe fondamental de responsabiliser les détenteurs de données personnelles en les obligeant à rapporter la preuve qu'ils ont respecté la loi, sous peine de lourdes sanctions.
- Pour être en conformité, notre entreprise devra suivre les 5 grands principes du RGPD. Que ce soit la proportionnalité et pertinence des données, le principe d'une durée limitée de conservation des données, le principe de sécurité, d'intégrité et de confidentialité des données, le principe d'interdiction de traitement de données dites sensibles ou encore le consentement des personnes.
- Tous les principes cités ci-dessus sont classés par ordre de priorité à mettre en place.

Les 5 principes du RGPD

Principe de proportionnalité et pertinence des données

- Le principe de proportionnalité, de pertinence et de minimisation des données est le principe selon lequel nous devons garder uniquement les données utiles à l'entreprise. Nous avons trouvé plusieurs données que nous considérons comme non pertinentes à collecter par l’entreprise, dans la partie “Identification de l’employé”, les catégories “profession des parents de l’employé” et “nature des études suivies par les enfants” ne nous semblent pas pertinentes. En cas de contrôle de la CNIL, notre entreprise devra justifier leurs utilisations.

Les 5 principes du RGPD

Principe d'une durée limitée de conservation des données

- Chacune des données collectées a une date limite de conservation qui fluctue en fonction du type de données. Tout d’abord les données de types vidéo qui peuvent être conservées pendant 1 mois.
- Les données de type documents comptables et les pièces justificatives sont conservés pendant 10 ans à compter de la date de la clôture de l’exercice.
- Les données de type contrat qui prévoit que l’employeur conserve un double des bulletins de paie des salariés ou des bulletins de paie remis aux salariés sous forme électronique pendant 5 ans.

Les 5 principes du RGPD

Principe de sécurité, d'intégrité et de confidentialité des données

- Pour bien commencer, l’intégrité d’une donnée correspond à l'exactitude, l'exhaustivité et aux cohérences globales des données.
- Mais plus concrètement pour notre entreprise, plusieurs choses sont à mettre en place comme :
- La documentation des procédures d’exploitation, les tenir à jour et les rendre disponibles à tous les utilisateurs concernés, la rédaction d'une charte informatique et lui donner une force contraignante.
- Pour plus d’informations ou pour quelconques renseignements, se renseigner auprès du DPO, chargé de la mise en pratique du RGPD au sien de l'entreprise.

Les 5 principes du RGPD

Principe d'interdiction de traitement de données dites sensibles

- Pour commencer notre entreprise traite des données à caractère sensible qui sont toutes informations se rapportant à une personne physique identifiée et identifiable.
- Nous avons pu en identifier plusieurs comme “nombre de jours de grève suivis”, “appartenance syndicale” ou encore “sanctions disciplinaires à l'exclusion de celles consécutives à des faits amnistiés”. Il y aussi le “taux d’invalidité” qui peut être considéré comme une donnée sensible si ce dernier n'est pas lié au travail. Toutes ces données sensibles citées ci-dessus peuvent être collectées par l’entreprise mais ne pourront être soumises à aucun traitement (toutes opérations effectuées à l’aide d’un procédé informatique et appliquées à des données personnelles).

Les 5 principes du RGPD

Principe de consentement des personnes

- Pour que notre entreprise soit conforme, il faut que toute personne au sien de l’entreprise signe une charte de connaissance et d’information informatique de collecte de donnée. Pour faire valoir de consentement sur les traitements de données sensibles et ou les traitements à des fins de prospection.
- De plus tous les employeurs ont accès à leur droit de rectification ce qui leur permet à tout moment le droit de rectifier, modifier, limiter ou supprimer leurs informations personnelles.

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

- La CNIL a été créé avec la loi du 6 janvier 1978 et réellement active à partir de la mise en place du RGPD le 25 mai 2018.
- La CNIL est une autorité administrative indépendante française. Elle est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
- La CNIL conseille et renseigne les personnes et les organismes, établit et publie aussi des lignes directrices, recommandations ou référentiels. Par ailleurs, la CNIL édite des règlements et reçoit les réclamations, pétitions et plaintes de salariés ou de syndicats. De plus, les agents de contrôle de la CNIL peuvent recueillir sur place ou sur convocation tout renseignement et toute justification utile et demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Les agents peuvent même utiliser une identité d'emprunt.

Définir un délégué à la protection des données (DPO)

- La désignation d'un délégué est obligatoire pour les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle. Ce qui est le cas dans notre entreprise.
- Dans notre entreprise, le délégué doit être désigné sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données. Si notre entreprise n'a pas de personne qualifiée pour devenir DPO, elle peut se renseigner auprès d'autres entreprises du domaine afin de mutualiser le DPO. Il doit être désigné par notre entreprise, par le responsable de traitement, et déclaré directement sur le site de la CNIL, par l'intermédiaire d'un formulaire en ligne.

Définir un délégué à la protection des données (DPO)

- Le délégué que vous aurez choisi devra se charger d’informer et de conseiller le responsable de traitement, le directeur, de contrôler le respect de la règlementation, de conseiller l’organisme sur la réalisation d’une analyse d'impact relative à la protection des données , de coopérer avec l’autorité de contrôle et d’être le point de contact des personnes concernées.
- Le délégué n’est pas personnellement responsable en cas de non-conformité de l'entreprise avec le règlement. C’est le responsable du traitement qui est tenu de s’assurer et être en mesure de démontrer que le traitement est effectué conformément à la règlementation.

Le Registre des Activités de Traitement

- Nous pouvons recommander à notre entreprise, et plus précisément au responsable de traitement, de mettre en place un Registre des Activités de Traitement. C’est un registre dans lequel il faut donc y renseigner tous les traitements de données à caractère personnel effectués par l’entreprise, autrement dit tous les traitements liés à l’identification d’un employé ainsi qu'au suivi de sa carrière et de sa formation. Il faut aussi, pour chaque traitement, y expliquer la sécurité mise en œuvre, l’utilité de la récolte de ces données personnelles, et justifier la collecte des données sensibles présentes au sein du système d'information.

Les différentes sanctions

- **Sanctions pénales :** Des peines jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende en cas de non-respect du principe de finalité et en cas de conservation de données sensibles sans le consentement exprès de l'intéressé
- **Sanctions administratives :**
  - Avertissement
  - Mise en demeure
  - Imposer de supprimer des données à caractère personnel
  - Ordonner au responsable du traitement ou au sous-traitant de se mettre en conformité avec le RGPD
  - Amendes administratives : 4% CA mondial annuel total ou 20 millions € d'amende maximum.
- **Sanctions civiles :** Toute personne qui subit un préjudice lié à une fuite de données à caractère personnel peut demander réparation au responsable de traitement sous forme de dommages-intérêts
- **Sanctions disciplinaires :** Licenciement du salarié pour faute grave

Sources

- Cours : Les principes à respecter
- Cours : La mise en œuvre concrète
- Cours : Les sanctions
- Cours : PPT des cours
- https://www.cnil.fr/fr