CONCOURS EXTERNE COMMUN ET CONCOURS INTERNE COMMUN POUR LE RECRUTEMENT DANS LE PREMIER GRADE DE DIVERS CORPS DE FONCTIONNAIRES DE CATÉGORIE B

Session 2018

Épreuve n° 1 : Cas pratique avec mise en situation à partir d'un dossier documentaire pouvant comporter des graphiques et des données chiffrées. Le dossier doit relever d'une problématique relative aux politiques publiques et comporter plusieurs questions précédées d'une présentation détaillée des attentes du jury destinées à mettre le candidat en situation de travail. (Dossier de 20 pages maximum).

Durée : 3 heures - Coefficient 3

Matériel :

L'usage de tout ouvrage de référence, de tout dictionnaire ou de tout matériel électronique (y compris la calculatrice) est rigoureusement interdit.

Consignes concernant les copies :

Les feuilles de brouillon fournies par l'administration ne doivent pas être insérées dans les copies et ne seront pas prises en compte dans la correction.

Vous devez rédiger avec un stylo dont l'encre est de couleur sombre.

Si vous utilisez plus d'une copie vous devez paginer votre composition correctement dans la zone en bas à droite de chacune des pages utilisées. Chaque pagination doit contenir le numéro de la page et le total des pages de votre composition (Ex : 1/8, 2/8, 3/8 etc.)

IMPORTANT

Assurez-vous que cet exemplaire est complet. S'il est incomplet, demandez en un autre aux surveillants.

Si un candidat repère ce qui semble être une erreur d'énoncé, il le signale sur sa copie et poursuit l'épreuve en conséquence.

Il vous est rappelé que votre identité ne doit figurer que dans la partie supérieure de la bande en-tête de la copie (ou des copies) mise(s) à votre disposition. Toute mention d'identité ou tout signe distinctif porté sur toute autre partie de la copie ou des copies que vous remettrez en fin d'épreuve entraînera l'annulation de votre épreuve.

Si la rédaction de votre devoir impose de mentionner des noms de personnes ou de villes et si ces noms ne sont pas précisés dans le sujet à traiter, vous utiliserez des lettres pour désigner ces personnes ou ces villes (A..., B..., Y..., Z...).

Ce document contient le sujet et comporte 20 pages, numérotées de 1 à 20.

Assurez-vous que cet exemplaire est complet. Dans le cas contraire, demandez-en un autre au responsable de la salle.

CAS PRATIQUE

Vous êtes secrétaire administratif (ve) au sein du bureau de la protection des mineurs en accueils collectifs et des politiques éducatives locales de la Direction de la jeunesse, de l'éducation populaire et de la vie associative (DJEPVA) du Ministère de l'éducation nationale.

Ce bureau organise la délivrance du brevet d'aptitudes aux fonctions d'animateur (BAFA) qui permet d'encadrer à titre non professionnel, de façon occasionnelle, des enfants et des adolescents en accueils collectifs de mineurs.

Les candidatures au brevet sont gérées via un site internet. Ce site a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour la collecte et le traitement de données personnelles conformément à la loi du 6 janvier 1978.
Un règlement européen de la protection des données personnelles (RGPD) entrera en vigueur à compter de mai 2018 et viendra modifier les règles en vigueur.

Votre chef de bureau vous demande de rédiger, à l'aide des éléments du dossier ci-joint, une note sur les impacts de ce nouveau règlement sur les droits des candidats et obligations de l'administration.

Vous répondrez en particulier aux questions suivantes :

- Qu'est-ce qu'une donnée personnelle ?
- Quels sont les principes fondamentaux renforcés par le règlement européen ?
- Quels seront les nouveaux droits des citoyens ?
- Quels sont les impacts en particulier pour votre chef de bureau, le responsable du traitement des données personnelles BAFA, données recueillies à partir du site internet ?

Documents joints (ce dossier contient 18 pages):

DOC 1 Plaquette d'information du brevet d'aptitude aux fonctions d'animateur - *(site internet* www.*jeunes.gouv.fr*/bafa-bafd - *janvier 2018)* page 3

DOC 2 « Obligations en matière de protection des données personnelles » *(site internet Service-public-pro.fr -article du 12/06/2017)* page 4

DOC 3 Article du 13/12/2017 – « Projet de loi relatif à la protection des données personnelles » *-(site internet Ministère de la Justice - décembre 2017)* page 5

DOC4 « Règlement européen sur la protection des données : se préparer en 6 étapes » *(Plaquette d'information de la CNIL – mars 2017)* pages 6 à 13

DOC 5 « Plus de droits pour vos données » *(Plaquette d'information de la CNIL – janvier 2016)* page 14

DOC 6 « Le règlement européen sur la protection des données vous concerne » *(RGPD Fiche 1 - Agence française de la santé numérique – novembre 2017)* pages 15 et 16

DOC 7 Extrait du règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) *(Journal officiel de l'union européenne)* pages 17 à 20

Document 1

Brevet d'animateur

Le Brevet d'aptitude aux fonctions d'animateur (BAFA) d'accueils collectifs de mineurs*, permet à ceux qui souhaitent s'engager dans une action éducative, d'encadrer des enfants et des adolescents à titre non professionnel, et de façon occasionnelle, dans ces accueils.

Pour l'obtenir, il faut avoir suivi avec succès les différentes étapes d'une formation, théorique et pratique, préparant le candidat à :

- assurer la sécurité physique et morale des mineurs et en particulier les sensibiliser, dans le cadre de la mise en œuvre d'un projet pédagogique, aux risques liés, selon les circonstances aux conduites addictives ou aux comportements, notamment ceux liés à la sexualité;
- participer à l'accueil, à la communication et au développement des relations entre les différents acteurs;
- participer, au sein d'une équipe, à la mise en œuvre d'un projet pédagogique en cohérence avec le projet éducatif dans le respect du cadre réglementaire des accueils collectifs de mineurs;
- encadrer et animer la vie quotidienne et les activités;
- accompagner les mineurs dans la réalisation de leurs projets.

Conditions d'accès à la formation

Le candidat doit avoir 17 ans révolus, sans possibilité de dérogation.

Modalité d'inscription

Le candidat doit s'inscrire, via le site internet www.jeunes.gouv.fr/bafa-bafd et choisir la direction départementale (DDCS ou DDCSPP) de son lieu de résidence.

Important : Ne pas oublier de transmettre une copie d'une pièce d'identité nationale recto/verso (carte d'identité, passeport...) à la direction départementale du lieu de résidence (DDCS - DDCSPP ou DJSCS) en pièce jointe via votre espace personnel internet www.jeunes.gouv.fr/bafa-bafd ou par courrier. En l'absence de production d'une pièce d'identité, le dossier ne pourra être présenté au jury en fin de cursus.

A propos de l'inscription en ligne

Déclaration Commission nationale de l'informatique et des libertés (Cnil) *du 24 avril 2009 : 1359202*
Propriétaire du site : Ministère de l'éducation nationale

Conformément à l'article 27 de la loi n°78-17 Informatique et Liberté du 06/01/1978, un droit d'accès, de modification, et de suppression des données des candidats est garanti. Pour l'exercer, il suffit d'adresser un courrier à la Direction de la jeunesse, de l'éducation populaire et de la vie associative (DJEPVA) 95, avenue de France 75650 Paris Cedex 13, en précisant nom, prénom et adresse.

Formation

La formation est composée de 3 étapes :
2 sessions théoriques et 1 stage pratique se déroulant obligatoirement dans l'ordre suivant :

1. Session de formation générale (8 jours) ;
2. Stage pratique (14 jours). Il est conseillé au candidat de commencer sa recherche de lieu de stage pratique en début de formation ;
3. Session d'approfondissement (6 jours) ou de qualification (8 jours).

Seules les sessions peuvent se dérouler à l'étranger. Les stages pratiques doivent se dérouler en France.

**autrefois appelés colonies de vacances et centres de loisirs, les accueils collectifs de mineurs reçoivent les enfants et les jeunes pour pratiquer des activités de loisirs éducatifs et de détente pendant les vacances et le temps de loisirs.*

Source : site internet du ministère de l'éducation nationale www.jeunes.gouv.fr/bafa-bafd - janvier 2018

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Service-Public-Pro.fr
Le site officiel de l'administration française

Fiche pratique

Obligations en matière de protection des données personnelles

Vérifié le 12 juin 2017 - Direction de l'information légale et administrative (Premier ministre), Ministère chargé de la justice

La création et le traitement de données personnelles (numéro d'identifiant, nom, adresse, numéro de téléphone...) sont soumis à des obligations destinées à protéger la vie privée des personnes fichées et les libertés individuelles. Elles varient selon la nature du fichier et la finalité des informations recueillies : déclaration normale ou simplifiée ou demande d'autorisation. Il existe aussi des obligations de sécurité, de confidentialité et d'information.

Déclaration

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés (Cnil) sous forme d'une :

- déclaration normale (https://www.service-public.fr/professionnels-entreprises/vosdroits/R1306) pour les fichiers qui concernent la vie privée ou les libertés individuelles des personnes : fichiers de clients, gestion des horaires des salariés, contrôle des accès aux locaux faisant l'objet d'une restriction de circulation, gestion de carrière et de la mobilité des salariés (organisation du travail, formations, annuaire interne, élections professionnelles, etc.), géolocalisation des véhicules utilisés par les salariés (ayant pour finalité le suivi et la facturation d'une prestation de transport, la sécurité des salariés ou des marchandises, le suivi du temps de travail, etc.) ;
- déclaration simplifiée (https://www.service-public.fr/professionnels-entreprises/vosdroits/R1384) valant engagement de conformité, pour les fichiers qui ne portent pas atteinte à la vie privée et aux libertés individuelles des personnes.

Par exemple, les sites commerciaux de vente en ligne de biens ou de services, qui collectent des informations nominatives (nom, courriel) et constituent des fichiers de clients et de prospects, doivent effectuer une déclaration simplifiée. En revanche, les traitements de données mis en œuvre à partir d'un site web, qui ne bénéficient ni d'une dispense, ni d'une procédure allégée, doivent faire l'objet d'une déclaration normale.

Pour savoir si un fichier doit être ou non déclaré et quelle procédure appliquer, il existe un service d'aide à la déclaration (https://www.service-public.fr/professionnels-entreprises/vosdroits/R18321) sur le site de la Cnil.

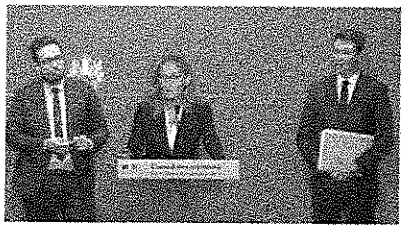
À savoir :
les formalités déclaratives doivent être effectuées par la personne responsable du fichier ou du traitement, celle qui en décide de la création et en détermine les finalités, **avant** la création du fichier.

13 décembre 2017

Projet de loi relatif à la protection des donnéespersonnelles

Le 13 décembre, Nicole Belloubet, garde des Sceaux, ministre de la Justice, a présenté en conseil des ministres le projet de loi relatif à la protection des données personnelles dont la mission est d'adapter la loi française Informatique et Libertés du6 janvier 1978 au droit européen.

« Le développement de l'ère numérique oblige à repenser le cadre applicable aux données personnelles » a énoncé Nicole Belloubet lors du compte rendu du conseil des ministres du 13 décembre 2017.



En mai 2018, la réglementation et la directive européenne sur la protection des données (RGPD) entreront en vigueur afin d'harmoniser ces mesures entre tous les pays de l'Union européenne. Le projet de loi porté par la ministre de la Justice en collaboration avec Mounir Mahjoubi, secrétaire d'État au numérique, transpose ce nouveau cadre juridique européen.

Ce projet de loi comporte des avancées majeures qui peuvent *«bouleverser les usages »* selon Mounir Mahjoubi. Le texte va créer un cadre unifié et protecteur pour les données personnelles tout en instaurant de nouveaux droits pour les citoyens, notamment un droit à la portabilité des données personnelles. *« La portabilité est une révolution »* a ajouté le secrétaire d'État au numérique.

Une simplification des règles auxquelles sont soumis les acteurs économiques sera également mise en place. Un contrôle a posteriori, fondé sur l'appréciation par le responsable de traitement des risques causés par son traitement remplacera le contrôle a priori, basé sur des déclarations et autorisations préalables. En contrepartie de cette responsabilisation des acteurs, les pouvoirs de la CNIL seront renforcés, comme les sanctions encourues qui pourront aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial consolidé. Toutefois le gouvernement a fait le choix de maintenir certaines formalités préalables pour les traitements des données les plus sensibles. *« On s'adapte en promoteur et non en suiveur »* a souligné la garde des Sceaux.

Les mineurs de moins de 16 ans seront mieux protégés : l'autorisation parentale sera nécessaire pour autoriser le traitement de leurs données. *« L'inscription sur Facebook supposera une autorisation parentale pour les mineurs de moins de 16 ans »* a expliqué Nicole Belloubet.

Enfin le texte renforce l'information des citoyens et leurs droits d'accès, de rectification et d'effacement des données.

Rappel

Les données personnelles correspondent à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (Article 2 de la loi informatique et liberté)

Source : Site internet institutionnel du Ministère de la justice
http://www.justice.gouv.fr/la-garde-des-sceaux-10016/projet-de-loi-relatif-a-la-protection-des-donnees-personnelles-31094.html

Document 4

Règlement européen

sur la protection des données personnelles

se préparer en 6 étapes

En mai 2018, le règlement européen sera applicable.
De nombreuses formalités auprès de la CNIL vont disparaître.
En contrepartie, la responsabilité des organismes sera renforcée.
Ils devront en effet assurer une protection optimale des données
à chaque instant et être en mesure de la démontrer
en documentant leur conformité.

Désigner
un pilote

Cartographier
vos traitements de
données personnelles

Prioriser
les actions

Gérer
les risques

Organiser
les processus internes

Documenter
la conformité

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

ÉTAPE 1

Désigner un pilote

Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exerce une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un correspondant Informatique et Libertés (CIL), qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener.

La désignation d'un délégué à la protection des données est obligatoire en 2018 si :

- **vous êtes un organisme public,**
- **vous êtes une entreprise** dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et à des infractions.

Même si votre organisme n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé de désigner une personne, disposant de relais internes, chargée de s'assurer de la mise en conformité au règlement européen. **Le délégué constitue un atout majeur pour comprendre et respecter les obligations du règlement, dialoguer avec les autorités de protection des données et réduire les risques de contentieux.**

Le rôle du délégué à la protection des données

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- **d'informer et de conseiller** le responsable de traitement ou le sous-traitant ainsi que leurs employés,
- **de contrôler le respect du règlement** et du droit national en matière de protection des données,
- **de conseiller l'organisme** sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution,
- **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci.

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

- informer sur le contenu des nouvelles obligations,
- sensibiliser les décideurs sur l'impact de ces nouvelles règles,
- réaliser l'inventaire des traitements de données de votre organisme,
- concevoir des actions de sensibilisation,
- piloter la conformité en continu.

Sur cnil.fr
Pour préparer la désignation de votre futur délégué, désignez un CIL.

Vous aurez franchi cette étape si :

- ☐ vous avez désigné au sein de votre structure un pilote (un CIL qui a vocation à être désigné délégué), chargé de mettre en œuvre la conformité au règlement sur la base d'une lettre de mission,
- ☐ vous lui avez affecté les moyens humains et financiers nécessaires pour mettre en œuvre ses missions.

Cartographier
vos traitements de données personnelles

Pour mesurer concrètement l'impact du règlement européen sur la protection des données de votre activité, commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. La tenue d'un registre des traitements vous permet de faire le point.

Dans le cadre du futur règlement, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du règlement sur votre activité et de répondre à cette exigence, vous devez au préalable recenser précisément :

- **les différents traitements** de données personnelles,
- **les catégories de données** personnelles traitées,
- **les objectifs poursuivis** par les opérations de traitement de données,
- **les acteurs** (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires sous-traitants,
- **les flux** en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Pour chaque traitement de données personnelles, posez-vous les questions suivantes :

QUI ?
- Inscrivez dans le registre le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données.
- Identifiez les responsables des services opérationnels traitant les données au sein de votre organisme.
- Etablissez la liste des sous-traitants.

QUOI ?
- Identifiez les catégories de données traitées.
- Identifiez les données susceptibles de soulever des risques en raison de leur sensibilité particulière (par exemple : les données relatives à la santé ou les infractions).

POURQUOI ?
Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données (par exemple : gestion de la relation commerciale, gestion RH...).

OÙ ?
- Déterminez le lieu où les données sont hébergées.
- Indiquez vers quels pays les données sont éventuellement transférées.

JUSQU'À QUAND ?
Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

COMMENT ?
Précisez les mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées.

Sur cnil.fr
Pour vous familiariser avec le futur registre des traitements de données personnelles, téléchargez notre modèle de registre.

Vous aurez franchi cette étape si :

- ☐ vous avez rencontré les services et les entités qui traitent des données personnelles,
- ☐ vous avez établi la liste des traitements par finalité principale (et non par outil ou applicatif utilisé) et les types de données traitées,
- ☐ vous avez identifié les sous-traitants qui interviennent sur chaque traitement,
- ☐ vous savez à qui et où les données sont transmises,
- ☐ vous savez où sont stockées vos données,
- ☐ vous savez combien de temps ces données sont conservées.

ÉTAPE 3

Prioriser les actions

Sur la base du registre des traitements de données personnelles, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées.

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de votre organisme, vous devez, pour chacun d'eux, identifier les actions à mener pour vous conformer aux obligations actuelles et à venir.

Cette priorisation peut être menée au regard des risques que font peser vos traitements sur les libertés des personnes concernées. Certaines tâches seront faciles à mettre en œuvre et vous permettront de progresser rapidement.

Points d'attention quels que soient les traitements de données

- **Assurez-vous** que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
- **Identifiez** la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- **Révisez** vos mentions d'information afin qu'elles soient conformes aux exigences du règlement.
- **Vérifiez** que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
- **Prévoyez** les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).
- **Vérifiez** les mesures de sécurité mises en place.

Points d'attention nécessitant une vigilance particulière

Vous traitez certains types de données :

- des données qui révèlent l'origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- des données relatives à la santé ou l'orientation sexuelle,
- des données génétiques ou biométriques,
- des données d'infraction ou de condamnation pénale,
- des données concernant des mineurs.

Votre traitement de données personnelles a pour effet :

- la surveillance systématique à grande échelle d'une zone accessible au public,
- l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Vous transférez des données hors de l'Union européenne ?

- Vérifiez que le pays vers lequel vous transférez les données est reconnu comme adéquat par la Commission européenne.
- Dans le cas contraire, encadrez vos transferts.

Sur cnil.fr

Pour préparer vos contrats avec vos sous-traitants, consultez notre modèle de clause de confidentialité.

Vous aurez franchi cette étape si :

- ☐ vous avez mis en place les premières mesures pour protéger les personnes concernées par vos traitements,
- ☐ vous avez identifié les traitements à risque.

Gérer les risques

Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données (en anglais, Privacy Impact Assessment ou PIA).

L'étude d'impact sur la protection des données permet :

- **de bâtir** un traitement de données personnelles ou un produit respectueux de la vie privée,
- **d'apprécier** les impacts sur la vie privée des personnes concernées,
- **de démontrer** que les principes fondamentaux du règlement sont respectés.

Quand mener une étude d'impact sur la protection des données (PIA) ?

- avant de collecter des données et de mettre en œuvre le traitement,
- sur tout traitement susceptible d'engendrer des risques élevés pour les droits et libertés des personnes physiques.

Que contient une étude d'impact sur la protection des données (PIA) ?

- **une description** du traitement et de ses finalités,
- **une évaluation** de la nécessité et de la proportionnalité du traitement,
- **une appréciation** des risques sur les droits et libertés des personnes concernées,
- **les mesures envisagées** pour traiter ces risques et se conformer au règlement.

Les outils pour vous aider

La CNIL met à votre disposition sur son site les guides PIA, catalogues de bonnes pratiques qui vous aide à déterminer les mesures proportionnées aux risques identifiés, en agissant sur :

- **les « éléments à protéger » :**
  minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits, etc.
- **les « impacts potentiels » :**
  sauvegarder les données, tracer l'activité, gérer les violations de données etc.
- **les « sources de risques » :**
  contrôler les accès, gérer les tiers, lutter contre les codes malveillants etc.
- **les « supports » :**
  réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier etc.

Pour traiter un risque identifié et le réduire à un niveau acceptable, l'utilisateur des guides peut sélectionner une ou plusieurs mesures appropriées. Il est impératif d'adapter les mesures au risque et au contexte particulier du traitement considéré. Des études de cas sur la géolocalisation de véhicules d'entreprise et la gestion des patients d'un cabinet de médecine du travail, réalisées par le Club EBIOS, illustrent la mise en application de ces outils.

Sur cnil.fr
Pour expérimenter la méthodologie du PIA, téléchargez les guides PIA de la CNIL.

Vous aurez franchi cette étape si :

- ☐ vous avez mis en place des mesures permettant de répondre aux principaux risques et menaces qui pèsent sur la vie privée des personnes concernées par vos traitements.

ÉTAPE 5

Organiser les processus internes

Pour garantir un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement de données personnelles (par exemple : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire etc.).

Organiser les processus implique notamment de :

- **prendre en compte** la protection des données personnelles dès la conception d'une application ou d'un traitement (minimisation de la collecte de données au regard de la finalité, cookies, durées de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données, s'assurer du rôle et de la responsabilité des acteurs impliqués dans la mise en œuvre de traitements de données) ; pour cela, appuyez-vous sur les conseils du délégué à la protection des données,
- **sensibiliser et d'organiser** la remontée d'information en construisant notamment un plan de formation et de communication auprès de vos collaborateurs,
- **traiter** les réclamations et les demandes des personnes concernées quant à l'exercice de leurs droits (droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement) en définissant les acteurs et les modalités (l'exercice des droits doit pouvoir se faire par voie électronique, si les données ont été collectées par ce moyen),
- **anticiper** les violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

Sur cnil.fr
Dans l'attente du téléservice de notification de violations de données personnelles (disponible en mai 2018 sur cnil.fr), consultez d'ores et déjà le formulaire de notification de violations de données personnelles.

Vous aurez franchi cette étape si :

- les réflexes de la protection des données sont acquis et appliqués au sein des services qui mettent en œuvre des traitements de données,
- votre organisme sait quoi faire et à qui s'adresser en cas d'incident.

ÉTAPE 6

Documenter la conformité

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les mesures organisationnelles et techniques sont réexaminées et actualisées si nécessaire.

Votre dossier devra notamment comporter les éléments suivants

La documentation sur vos traitements de données personnelles

- le registre des traitements (pour les responsables de traitements) ou des catégories d'activités de traitements (pour les sous-traitants),
- les analyses d'impact sur la protection des données (PIA ; voir étape 4) pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes,
- l'encadrement des transferts de données hors de l'Union européenne (notamment les clauses contractuelles types ou les BCR).

L'information des personnes

- les mentions d'information,
- les modèles de recueil du consentement des personnes concernées,
- les procédures mises en place pour l'exercice des droits des personnes.

Les contrats qui définissent les rôles et les responsabilités des acteurs

- les contrats avec les sous-traitants,
- les procédures internes en cas de violations de données,
- les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

Vous aurez franchi cette étape si :

- ☐ votre documentation démontre que vous respectez les obligations prévues par le règlement européen.

Les ressources

Désigner un pilote

> Le CIL et le futur délégué à la protection des données [PAGE WEB]
> Guide pratique de la prise de fonction du CIL [PDF]
> Devenir délégué à la protection des données [PAGE WEB]

Cartographier vos traitements

> Modèle de registre règlement européen [EXCEL]
> Exemple de fiche de registre CIL [PDF]
> Demandez la liste des fichiers déclarés à la CNIL [FORMULAIRE]

Prioriser les actions

> Guide sécurité des données personnelles [PDF]
> Modèle de clause de contrat de confidentialité [PDF]
> Modèle de clause de contrat de confidentialité sous-traitant pour maintenance ou télémaintenance [PDF]

Gérer les risques

> PIA-2, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée [PDF]
> PIA-3, les bonnes pratiques : Mesures pour traiter les risques sur les libertés et la vie privée [PDF]

Organiser les processus internes

> Le référentiel du label Gouvernance [DOCX]
> La notification de violations [PAGE WEB]

Retrouvez toutes les ressources dans la rubrique « Règlement européen » du site de la CNIL

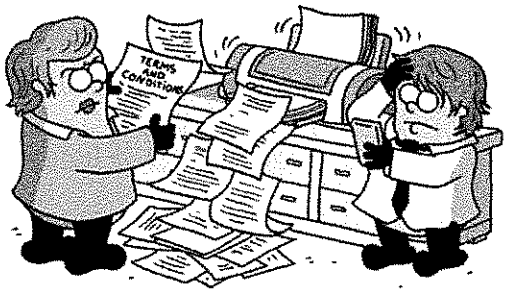
Plus de droits pour vos données !

1 Des données à emporter !

Je peux récupérer les données que j'ai communiquées à une plate-forme et les transmettre à une autre (réseau social, fournisseur d'accès à internet, site de streaming, etc.)

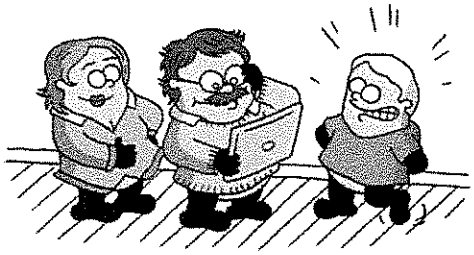
2 Plus de transparence

Je bénéficie de plus de lisibilité sur ce qui est fait de mes données et j'exerce mes droits plus facilement (droit d'accès, droit de rectification).



3 Protection des mineurs

Les services en ligne doivent obtenir le consentement des parents des mineurs de moins de 16 ans avant leur inscription.

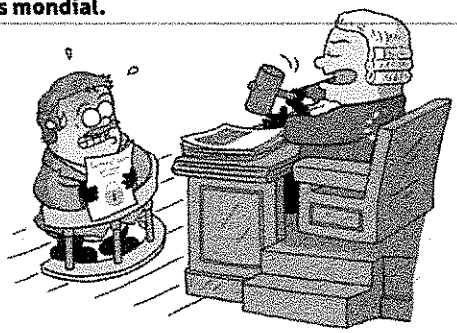


4 Guichet unique

En cas de problème, je m'adresse à l'autorité de protection des données de mon pays, quel que soit le lieu d'implantation de l'entreprise qui traite mes données.

5 Sanction renforcée

En cas de violation de mes droits, l'entreprise responsable encourt une sanction pouvant s'élever à 4% de son chiffre d'affaires mondial.



6 Consécration du droit à l'oubli

Je peux demander à ce qu'un lien soit déréférencé d'un moteur de recherche ou qu'une information soit supprimée s'ils portent atteinte à ma vie privée.

Illustration : Martin Vidberg

Nouveau Règlement européen sur la protection des données personnelles

Après quatre années de débats, l'Union européenne a finalisé le projet de règlement sur la protection des données personnelles qui doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Le règlement, qui sera adopté au premier semestre 2015, renforce les droits des citoyens européens et leur donne plus de contrôle sur leurs données personnelles. Il simplifie les formalités pour les entreprises et leur offre un cadre juridique unique. Il sera applicable en 2018 dans tous les pays de l'UE.

ARTICLE 29 Data Protection Working Party

CNIL

Document 6

Le règlement européen sur la protection des données personnelles (RGPD) vous concerne

EN BREF

- 25 mai 2018 : le règlement européen sur la protection des données personnelles (RGPD) s'applique à tous les organismes et dans tous les secteurs d'activité ;
- Son objectif : renforcer les droits des citoyens européens vis-à-vis de la protection de leurs données personnelles, dans un environnement numérique croissant et mondialisé ;
- Ses impacts : des formalités auprès de la CNIL sont remplacées par une responsabilisation accrue des organismes (et de leurs sous-traitants) qui doivent assurer une protection optimale des données à chaque instant, et être en mesure de la démontrer en documentant leur conformité. Les contrôles et les sanctions sont renforcés.

Un nouveau cadre juridique qui s'applique à tous dès mai 2018

Les données personnelles sont protégées en France par le **cadre juridique** de la loi n°78-17 du 6 janvier 1978 dite « loi Informatique et Libertés », qui **évolue** avec l'entrée en vigueur **en mai 2018** du règlement européen n°2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD).

Le RGPD est un texte européen, commun à tous les pays membres de l'Union européenne, **qui concerne tous les organismes**, tant publics que privés, **et tous les secteurs d'activité.**

Il renforce les droits des personnes et accroit les obligations des **responsables de traitement** et des **sous-traitants**.

Il s'applique aux **traitements de données personnelles**, réalisés sur **support informatique** (logiciels, applications, bases de données, sites web…), mais également sur **support papier**.

Le secteur de la santé est d'autant plus impacté par ce texte que les données de santé bénéficient d'un régime de protection renforcé, les données de santé étant considérées comme des données sensibles. A cela s'ajoutent les obligations additionnelles prévues par le code de la santé publique, relatives aux données de santé couvertes par le secret médical (règles relatives à l'hébergement externalisé des données de santé, télémédecine, identifiant national de santé, etc.).

Le RGPD instaure pour la première fois une définition des données de santé : « *Les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ». Il précise que les données de santé peuvent se rapporter à l'état de santé (passé, présent ou futur) d'une personne, par exemple les données collectées dans un contexte médical (prestation de soins de santé, résultats de tests,...), ainsi que les données permettant d'identifier une maladie ou un risque de maladie, un handicap, des antécédents médicaux, un traitement clinique, un état physiologique ou biomédical.
Les données génétiques et les données biométriques sont également définies par le RGPD.

Des obligations majeures renforcées et nouvelles

Le RGPD impose à tous les acteurs traitant des données personnelles, qu'ils soient responsables de traitement ou sous-traitants, **certaines obligations majeures**, dont ils doivent pouvoir **démontrer le respect à tout moment** :

R **La tenue d'un registre interne**, qui décrit les traitements mis en œuvre au sein de l'organisme. Les formalités déclaratives auprès de la CNIL étant supprimées, la mise en conformité d'un traitement de données personnelles passe principalement par la tenue de cette documentation interne (registre, analyse d'impact, audits réguliers…).
Dans certains cas, la mise en œuvre du traitement reste toujours soumise à l'autorisation préalable de la CNIL.

La tenue du registre devient **obligatoire pour tous**. Auparavant, seuls les organismes disposant d'un correspondant informatique et libertés (CIL) devaient tenir cette documentation des traitements.

R **La désignation d'un délégué à la protection des données (DPD ou DPO)**, désormais obligatoire pour les organismes publics ainsi que pour tout organisme mettant en œuvre des traitements créant des risques particuliers pour les personnes (par exemple le suivi des personnes ou le traitement de données sensibles - telles des données de santé - à grande échelle). Le DPD est chargé d'informer et de conseiller son organisme sur ses obligations, de contrôler le respect du RGPD et du droit national et de coopérer avec l'autorité de contrôle. La mutualisation d'un DPD pour plusieurs organismes est possible.

La désignation d'un DPD, qui remplace le CIL dont la désignation était facultative, **devient obligatoire pour de nombreux organismes** (tous les organismes publics et autres organismes dont l'activité est décrite à l'article 47 du RGPD).

La sécurisation juridique, technique et organisationnelle des traitements, impliquant notamment :

- N la **mise en œuvre de processus** permettant d'assurer la sécurité et la confidentialité des données, ainsi que le respect des droits des personnes (procédures internes, mentions et processus d'information, clauses contractuelles avec les sous-traitants et les partenaires, adhésion à des codes de conduites, réalisation de certifications…)
- N la réalisation d'un **document d'analyse de l'impact du traitement de données sur la vie privée** pour les personnes avant certains traitements sensibles.

R **L'intégration des problématiques liées aux données personnelles dès le début d'un projet** : le RGPD impose de prendre en compte les principes de protection des données personnelles dès la conception d'un système d'information (« *Privacy by design* »), et dans le paramétrage par défaut de ces systèmes (« *Privacy by default* »).

Préparer son organisme dès à présent

L'entrée en vigueur du RGPD implique ainsi un renforcement des obligations pour tous les organismes, qui s'accompagne d'un rehaussement des sanctions applicables en la matière ainsi que d'une meilleure compréhension pour les personnes des droits dont elles disposent concernant leurs données personnelles.

Les impacts du RGPD s'étudient dans la continuité des actions d'ores et déjà portées par l'organisme pour gérer sa conformité juridique et les risques de sécurité de son système d'information.

Pour plus d'informations :

- ***CNIL : Le règlement européen n°2016/679 du 27 avril 2016 sur la protection des données personnelles (RGPD)*** www.cnil.fr/fr/reglement-europeen-protection-donnees
- ***CNIL : Comprendre le règlement européen*** www.cnil.fr/fr/comprendre-le-reglement-europeen
- ***CNIL : Ce qui change pour les professionnels*** www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels
- ***CNIL : Se préparer en 6 étapes*** www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

R Obligation renforcée

N Nouvelle exigence

Ce document est la propriété de l'ASIP Santé - Son utilisation, sa reproduction ou sa diffusion sans l'autorisation préalable et écrite de l'ASIP Santé sont interdites.

4.5.2016

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,
vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la proposition de la Commission européenne, après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen,

vu l'avis du Comité des régions,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit :

(1) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. L'article 8, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte») et l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne disposent que toute personne a droit à la protection des données à caractère personnel la concernant.

(2) Les principes et les règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel les concernant devraient, quelle que soit la nationalité ou la résidence de ces personnes physiques, respecter leurs libertés et droits fondamentaux, en particulier leur droit à la protection des données à caractère personnel. Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.

(3) La directive 95/46/CE du Parlement européen et du Conseil vise à harmoniser la protection des libertés et droits fondamentaux des personnes physiques en ce qui concerne les activités de traitement et à assurer le libre flux des données à caractère personnel entre les États membres.

(4) Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique.

(5) L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation substantielle des flux transfrontaliers de données à caractère personnel. Les échanges de données à caractère personnel entre acteurs publics et privés, y compris les personnes physiques, les associations et les entreprises, se sont intensifiés dans l'ensemble de l'Union. Le droit de l'Union appelle les autorités nationales des États membres à coopérer et à échanger des données à caractère personnel, afin d'être en mesure de remplir leurs missions ou d'accomplir des tâches pour le compte d'une autorité d'un autre État membre.

(6) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

(7) Ces évolutions requièrent un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. Les personnes physiques devraient avoir le contrôle des données à caractère personnel les concernant. La sécurité tant juridique que pratique devrait être renforcée pour les personnes physiques, les opérateurs économiques et les autorités publiques.

(8) Lorsque le présent règlement dispose que le droit d'un État membre peut apporter des précisions ou des limitations aux règles qu'il prévoit, les États membres peuvent intégrer des éléments du présent règlement dans leur droit dans la mesure nécessaire pour garantir la cohérence et pour rendre les dispositions nationales compréhensibles pour les personnes auxquelles elles s'appliquent.

(9) Si elle demeure satisfaisante en ce qui concerne ses objectifs et ses principes, la directive 95/46/CE n'a pas permis d'éviter une fragmentation de la mise en œuvre de la protection des données dans l'Union, une insécurité juridique ou le sentiment, largement répandu dans le public, que des risques importants pour la protection des personnes physiques subsistent, en particulier en ce qui concerne l'environnement en ligne. Les différences dans le niveau de protection des droits et libertés des personnes physiques, en particulier le droit à la protection des données à caractère personnel, à l'égard du traitement des données à caractère personnel dans les États membres peuvent empêcher le libre flux de ces données dans l'ensemble de l'Union. Ces différences peuvent dès lors constituer un obstacle à l'exercice des activités économiques au niveau de l'Union, fausser la concurrence et empêcher les autorités de s'acquitter des obligations qui leur incombent en vertu du droit de l'Union. Ces différences dans le niveau de protection résultent de l'existence de divergences dans la mise en œuvre et l'application de la directive 95/46/CE.

(10) Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées «données sensibles»). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite.

(11) Une protection effective des données à caractère personnel dans l'ensemble de l'Union exige de renforcer et de préciser les droits des personnes concernées et les obligations de ceux qui effectuent et déterminent le traitement des données à caractère personnel, ainsi que de prévoir, dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations.

(12) L'article 16, paragraphe 2, du traité sur le fonctionnement de l'Union européenne donne mandat au Parlement européen et au Conseil pour fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ainsi que les règles relatives à la libre circulation des données à caractère personnel.

(13) Afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micro, petites et moyennes entreprises, pour offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants, et pour assurer une surveillance cohérente du traitement des données à caractère personnel, et des sanctions équivalentes dans tous les États membres, ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres. Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Pour tenir compte de la situation particulière des micro, petites et moyennes entreprises, le présent règlement comporte une dérogation pour les organisations occupant moins de 250 employés en ce qui concerne la tenue de registres. Les institutions et organes de l'Union, et les États membres et leurs autorités de contrôle sont en outre encouragés à prendre en considération les besoins spécifiques des micro, petites et moyennes entreprises dans le cadre de l'application du présent règlement. Pour définir la notion de micro, petites et moyennes entreprises, il convient de se baser sur l'article 2 de l'annexe de la recommandation 2003/361/CE de la Commission.

(14) La protection conférée par le présent règlement devrait s'appliquer aux personnes physiques, indépendamment de leur nationalité ou de leur lieu de résidence, en ce qui concerne le traitement de leurs données à caractère personnel. Le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale.

(15) Afin d'éviter de créer un risque grave de contournement, la protection des personnes physiques devrait être neutre sur le plan technologique et ne devrait pas dépendre des techniques utilisées. Elle devrait s'appliquer aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier. Les dossiers ou ensembles de dossiers de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent règlement.

(16) Le présent règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale. Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union.

(17) Le règlement (CE) no 45/2001 du Parlement européen et du Conseil s'applique au traitement des données à caractère personnel par les institutions, organes et organismes de l'Union. Le règlement (CE) no 45/2001 et les autres actes juridiques de l'Union applicables audit traitement des données à caractère personnel devraient être adaptés aux principes et aux règles fixés dans le présent règlement et appliqués à la lumière du présent règlement. Pour mettre en place un cadre de protection des données solide et cohérent dans l'Union, il convient, après l'adoption du présent règlement, d'apporter les adaptations nécessaires au règlement (CE) no 45/2001 de manière à ce que celles-ci s'appliquent en même temps que le présent règlement.

(18) Le présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques.

(19) La protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil. Les États membres peuvent confier à des autorités compétentes au sens de la directive (UE) 2016/680 des missions qui ne sont pas nécessairement effectuées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, de manière à ce que le traitement de données à caractère personnel à ces autres fins, pour autant qu'il relève du champ d'application du droit de l'Union, relève du champ d'application du présent règlement.

En ce qui concerne le traitement de données à caractère personnel par ces autorités compétentes à des fins relevant du champ d'application du présent règlement, les États membres devraient pouvoir maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement. Ces dispositions peuvent déterminer plus précisément les exigences spécifiques au traitement de données à caractère personnel par ces autorités compétentes à ces autres fins, compte tenu de la structure constitutionnelle, organisationnelle et administrative de l'État membre concerné. Lorsque le traitement de données à caractère personnel par des organismes privés relève du champ d'application du présent règlement, celui-ci devrait prévoir la possibilité pour les États membres, sous certaines conditions, de limiter par la loi certaines obligations et certains droits lorsque cette limitation constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir des intérêts spécifiques importants tels que la sécurité publique, ainsi que la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. Cela est pertinent, par exemple, dans le cadre de la lutte contre le blanchiment d'argent ou des activités des laboratoires de police scientifique.

(20) Bien que le présent règlement s'applique, entre autres, aux activités des juridictions et autres autorités judiciaires, le droit de l'Union ou le droit des États membres pourrait préciser les opérations et procédures de traitement en ce qui concerne le traitement des données à caractère personnel par les juridictions et autres autorités judiciaires. La compétence des autorités de contrôle ne devrait pas s'étendre au traitement de données à caractère personnel effectué par les juridictions dans l'exercice de leur fonction juridictionnelle, afin de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions judiciaires, y compris lorsqu'il prend des décisions. Il devrait être possible de confier le contrôle de ces opérations de traitement de données à des organes spécifiques au sein de l'appareil judiciaire de l'État membre, qui devraient notamment garantir le respect des règles du présent règlement, sensibiliser davantage les membres du pouvoir judiciaire aux obligations qui leur incombent en vertu du présent règlement et traiter les réclamations concernant ces opérations de traitement de données.

(21) Le présent règlement s'applique sans préjudice de l'application de la directive 2000/31/CE du Parlement européen et du Conseil, et notamment du régime de responsabilité des prestataires de services intermédiaires prévu dans ses articles 12 à 15. Cette directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

(22) Tout traitement de données à caractère personnel qui a lieu dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union devrait être effectué conformément au présent règlement, que le traitement lui-même ait lieu ou non dans l'Union. L'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue pour un tel dispositif, qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique, n'est pas déterminante à cet égard.

(23) Afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du présent règlement, le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait être soumis au présent règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Afin de déterminer si un tel responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union. Alors que la simple accessibilité du site internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union.

(24) Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union devrait également être soumis au présent règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.

(25) Lorsque le droit d'un État membre s'applique en vertu du droit international public, le présent règlement devrait s'appliquer également à un responsable du traitement qui n'est pas établi dans l'Union, par exemple qui se trouve auprès de la représentation diplomatique ou consulaire d'un État membre.

(26) Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche.

(27) Le présent règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Les États membres peuvent prévoir des règles relatives au traitement des données à caractère personnel des personnes décédées.

(28) La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données.

(29) Afin d'encourager la pseudonymisation dans le cadre du traitement des données à caractère personnel, des mesures de pseudonymisation devraient être possibles chez un même responsable du traitement, tout en permettant une analyse générale, lorsque celui-ci a pris les mesures techniques et organisationnelles nécessaires afin de garantir, pour le traitement concerné, que le présent règlement est mis en œuvre, et que les informations supplémentaires permettant d'attribuer les données à caractère personnel à une personne concernée précise soient conservées séparément. Le responsable du traitement qui traite les données à caractère personnel devrait indiquer les personnes autorisées à cet effet chez un même responsable du traitement.

(30) (...)