Les lignes de force du Règlement général sur la protection des données

« Nous appelons homme libre celui qui est à lui-même sa fin et n'est pas la fin d'autrui ».

Aristote, *Métaphysique*

EMMANUEL JOUFFIN

Docteur en droit
Responsable juridique de banque

Le Règlement 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 (ci-après RGPD) a été publié au Journal officiel de l'Union européenne le 4 mai 2016[1]. Ce texte abroge la directive 95/46/CE, mais en conserve les principes essentiels tout en les revisitant de manière approfondie. Il en découle des impacts opérationnels significatifs.

Ce texte, qui marque le début d'une période transitoire de 2 ans[2] destinée à permettre aux responsables de traitements de se mettre en conformité avec leurs nouvelles obligations, repose sur trois piliers. Tout d'abord, renforcer les droits des personnes (notamment au travers de la portabilité des données personnelles et de dispositions spécifiques aux mineurs), mettre les responsables de traitement et sous-traitants face à leurs responsabilités au travers du principe d'*accountability* et, enfin, renouveler la coopération avec les autorités de protection des données, ces dernières disposant d'un pouvoir de sanction très significatif.

I. LES POINTS CLÉS DU RGPD

Si, globalement, les principes posés par la Directive 95/46 et la loi Informatique et Libertés demeurent, le Règlement les revisite et introduit de nouveaux principes.

1. L'*accountability*[3]

Cette notion constitue une des innovations majeures introduites par le RGPD. L'*accountability* conduit à l'émergence d'une gouvernance renforcée du cycle de vie des produits et services et des données personnelles qui y sont associées. L'*accountability* manifeste la bascule d'un mécanisme de formalités préalables[4] à un mécanisme d'autocontrôle[5] dans lequel lesdites formalités ont quasiment disparu[6]. Le but est de mettre à la charge des responsables de traitement la démonstration, tout au long du cycle de vie des données personnelles, du respect des dispositions protectrices de celles-ci.

Point d'attention

La protection des données n'est plus un état figé mais un ensemble dynamique de procédures. L'article 24 du RGPD impose à l'entreprise de mettre « *en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au [présent] règlement* ». Il faudra disposer de documents auditables au sujet des mesures prises pour maintenir et piloter la conformité ; cette disposition inclut le recensement, dans un registre interne, des traitements mis en œuvre[7].

2. *Privacy impact assessment* (PIA) ou étude d'impact sur la vie privée (EIVP)

Seul vestige des autorisations préalables, cette étude est nécessaire pour les traitements comportant des risques

1. Règlement n° 2016-679 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) du 27 avril 2016 JOUE du 4 mai 2016.
2. Le Règlement sera applicable le 25 mai 2018 (art. 99 du Règlement).
3. On se reportera à l'avis du G29 du 13 juillet 2010 relatif à l'*accountability* : http://www.cnpd.public.lu/fr/publications/groupe-art29/wp173_fr.pdf.
4. Déclarations, demandes d'autorisation réalisées auprès du régulateur préalablement à la mise en œuvre d'un nouveau traitement de données. Bien que ces formalités préalables aient été déjà allégées depuis la mise en place du Correspondant Informatique et Libertés dans les entreprises.
5. Le considérant 89 du règlement évoque explicitement l'échec de la protection des données telle qu'envisagée par la directive 95/46 fondée sur la réalisation de formalités préalables.
6. Le seul cas est l'autorisation de la CNIL lorsque l'étude d'impact conduite par l'entreprise laisse apparaitre que le traitement projeté comporte des risques importants pour la vie privée des individus.
7. Tout ceci évoque les exigences des orientations de l'ABE en matière de gouvernance des produits de banque de détail : cf. cette revue, chronique « Régulation et conformité ».

particuliers pour les personnes[8]. Cette analyse a pour épicentre, non pas les intérêts de l'entreprise, mais les risques que présente un nouveau traitement pour les personnes concernées[9].

Point d'attention

L'analyse d'impact doit comprendre[10], outre une description des opérations de traitement et de leurs finalités, une évaluation de ces opérations au regard de la finalité poursuivie et des risques pour les individus, ainsi qu'une description des mesures de protection envisagées. La consultation de l'autorité de contrôle n'est obligatoire qu'en présence d'un risque élevé qui ne peut-être atténué par des moyens raisonnables (cf. considérant 94 du RGPD). Lorsque l'autorité de contrôle estime que le traitement envisagé représente un risque, celle-ci fournit par écrit, dans un délai maximum de huit semaines[11] à compter de la réception de la demande de consultation, un avis au responsable du traitement, voire au sous-traitant[12]. Les délais d'examen de la demande peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations demandées. L'article 35-4 prévoit que l'autorité de contrôle publie une liste des types de traitement nécessitant une EIVP.

3. *Privacy by design et privacy by default*

Ce principe est fondé sur le fait que la protection de la vie privée doit être prise en considération, dès la phase de conception et de spécification des offres avec la nécessité de tenir compte de principes tels que : proportionnalité et pertinence des données collectées, durée de conservation, mesures de sécurité telles que le chiffrement des bases, etc[13].

Non seulement l'entreprise doit prendre en considération les enjeux liés à la protection des données dès l'origine, mais elle doit en outre être en mesure de démontrer que les traitements qu'elle met en œuvre respectent le cadre légal (mise en place de processus organisationnels et tenue du registre des traitements). Le principe de « *privacy by default* » exige quant à lui que les technologies et les procédures protectrices de la vie privée soient activées, par défaut, afin de procurer une protection la plus élevée possible.

4. Codes de conduite et Certification

Leur adoption a pour objet de minimiser les sanctions de l'autorité de contrôle en cas de défaut de conformité au RGPD. Ces codes de conduite, issus d'associations ou de syndicats professionnels, ont vocation à déterminer des pratiques destinées à la bonne application des obligations issues du RGPD[14]. Ils peuvent être soumis et, le cas échéant, approuvés par la Commission européenne[15].

La certification[16] réside quant à elle dans une démarche volontaire par laquelle l'entreprise fait constater la conformité de ses procédures à une norme avalisée par l'autorité de contrôle. Contrairement aux codes de conduites, la certification ne peut être délivrée que par un organisme de certification, celui-ci ayant été au préalable agréé par l'autorité de contrôle.

Point d'attention

La certification doit permettre une évaluation rapide du niveau de protection des données. Il conviendra de déterminer les produits et services pour lesquels il est nécessaire de la mettre en place. Cette démarche n'est pas à prendre à la légère. D'une part, le RGPD tient compte de l'adoption de tels dispositifs en tant que circonstance permettant une modulation à la baisse d'une éventuelle sanction[17]. D'autre part, la violation de telles normes serait de nature à engager la responsabilité professionnelle des contrevenants à l'égard de l'Autorité de Contrôle Prudentiel et de Résolution[18]. Un référentiel de ces labels serait souhaitable, de même qu'une procédure d'agrément des certificateurs.

5. Aggravation des sanctions

L'article 83 du RGPD renforce considérablement les sanctions[19]. Les amendes administratives prévues par le RGPD peuvent s'élever à 20 millions d'euros et, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[20].

Les sanctions sont modulables. L'autorité de contrôle pourra tenir compte des « *avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation* »[21], ce qui constitue une introduction larvée de la prise en compte de la faute lucrative. L'article 83 du RGPD vise par ailleurs un ensemble d'éléments relatifs au comportement du responsable du traitement, ses antécédents, sa collaboration de bonne foi avec l'autorité de contrôle, l'adoption et l'application de codes de conduites ou de labels.

8. Article 35 et 36 du RGPD : Scoring, données sensibles, vidéosurveillance, données génétiques ou biométriques, usage de nouvelles technologies
9. Il s'agit donc plus d'une sorte d'autocritique de ses nouveaux projets par l'entreprise.
10. Article 36-3 du RGPD.
11. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement. En cas de prolongation du délai, l'autorité en informe le responsable du traitement dans un délai d'un mois à compter de la réception de la demande de consultation - Art. 36-2.
12. A cette occasion, l'autorité peut utiliser les pouvoirs d'enquête de l'article 58 du RGPD.
13. Concept apparu au Canada en 2012 : http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf
14. Art. 40 du RGPD.
15. Art. 40 7° du RGPD.
16. Art. 42 du RGPD. Sur la notion de certification et ses implications, O. Tambou, « L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ? », RLDI, n° 126, mai 2016, p 43
17. Art 83-2 j vise « *l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42* ».
18. L'arrêté du 3 novembre 2014 abrogeant le règlement CRBF 97/02 évoque dans un article 10 P le risque de de non-conformité en mentionnent notamment le non-respect de normes professionnelles et déontologiques, rédaction identique à celle de l'article 4 P du défunt CRBF 97/02.
19. Art. 47 de la loi informatique et libertés : amende est de 150 000 euros pour un premier manquement et de 300 000 euros en cas de réitération ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de 300 000 euros.
20. Art. 83-5 du RGPD. Sont notamment concernés les manquements en matière de droit des personnes, de transferts de données hors UE et de licéité des traitements. L'article 83-4 vise des amendes d'un montant maximum de 10 millions d'euros ou, dans le cas d'une entreprise, « *jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu* ». Sont notamment visés par ces sanctions les manquements relatifs au consentement des mineurs, aux obligations « générales » du responsable du traitement en termes de tenue du registre des traitements, aux notifications de violations, à la conduite des études d'impacts et à la consultation du délégué à la protection des données.
21. Art. 83-2 k. du Règlement.

Le périmètre de la sanction est étendu. Le RGPD vise les « entreprises »[22] dont l'arrêt *Höfner*[23] livre une définition concernant le droit de la concurrence : « *dans le contexte du droit de la concurrence, la notion d'entreprise comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement* »[24]. Cette référence faite par le RGPD au droit de la concurrence n'étant pas pertinente s'agissant de données personnelles, une clarification sur ce sujet serait la bienvenue. La question de la manière dont seront « transposés », notamment par la CNIL, des critères retenus en droit de la concurrence afin de déterminer l'entité responsable de pratiques anticoncurrentielles revêt un enjeu très important.

Se posera rapidement la question du cumul des amendes qui pourront être prononcées par l'autorité de contrôle, avec d'autres sanctions administratives prononcées par les superviseurs bancaires, voire pénales par le juge. Par ailleurs, la procédure devant l'autorité de contrôle devra faire l'objet d'une grande attention. S'il a été jugé que l'article 6 CEDH ne s'applique qu'à la procédure de sanction, et non au niveau du contrôle, c'est sous réserve qu'il ne soit pas porté irrémédiablement atteinte aux droits de la défense[25]. On souhaite que la CNIL se dote d'une charte d'enquête[26] prenant notamment position sur l'information relative à l'assistance d'un avocat au cours desdites enquêtes.

6. Principe de responsabilité des sous-traitants

Le RGPD introduit une responsabilité des sous-traitants[27] à l'égard des données qu'ils traitent alors que, jusqu'ici, seuls les responsables de traitement étaient soumis aux obligations de la loi informatiques et libertés ainsi qu'aux sanctions pénales et administratives prévues par cette dernière.

Plus que jamais, le responsable de traitement ne doit faire appel qu'à des sous-traitants présentant des garanties suffisantes pour la mise en œuvre du RGPD.

Point d'attention

La question de l'application des dispositions de l'arrêté du 3 novembre 2014 relatif au contrôle interne[28] se posera avec acuité, y compris bien entendu dans sa dimension audit des sous-traitants. À cet égard, se posera la question de la qualification de prestations de service essentielles externalisées s'agissant des tâches confiées à ces derniers et ce, au regard du type de données, des catégories des personnes concernées[29]. Au terme du contrat, le RGPD prévoit que le sous-traitant doit supprimer les données personnelles et leurs éventuelles copies[30].

7. Reconnaissance de l'intérêt légitime du responsable de traitement

Le RGPD reconnaît la licéité de principe d'un traitement en présence d'un l'intérêt légitime du responsable de traitement[31]. Entrent dans le cadre de cet intérêt légitime, la lutte anti-fraude, le marketing direct, l'échange de données clients ou d'informations administratives intra-groupe[32].

Cette licéité de principe est toutefois soumise à conditions. Tout d'abord, il convient de tenir compte des intérêts et droits fondamentaux des personnes concernées, « *compte tenu des attentes raisonnables des personnes concernées fondées sur leur relation avec le responsable du traitement* », à l'égard de la possibilité d'un traitement ultérieur[33]. La question est de savoir ce qu'est une attente raisonnable, notion variable d'un individu à l'autre.

La prudence dicte d'être transparent sur les finalités du traitement. En présence d'un groupe d'entreprises, la transmission de données à caractère personnel au sein de ce groupe « *à des fins administratives internes, y compris le traitement de données à caractère personnel relatives à des clients ou des employés* » est évoquée au titre des intérêts légitimes.

Point d'attention

En l'absence de liste exhaustive de traitements constituant un intérêt légitime, il appartiendra au responsable de traitement de justifier de l'application de l'article 5.b du RGPD, lequel énonce que les données doivent être traitées en vue de « *finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités…* ».

Le G29, dans une opinion consacrée à la limitation de la finalité des traitements[34], souligne que celle-ci s'entend d'amont en aval[35]. La définition de la finalité

22. Le considérant 150 précise : « *Lorsque des amendes administratives sont imposées à une entreprise, ce terme doit, à cette fin, être compris comme une entreprise conformément aux articles 101 et 102 du traité sur le fonctionnement de l'Union européenne* ». Ces textes concernent les pratiques anticoncurentielles. L'article 4-18 donne de l'« *entreprise* » une définition guère éclairante : « *une personne physique ou morale exerçant une activité économique, quelle que soit sa forme juridique, y compris les sociétés de personnes ou les associations qui exercent régulièrement une activité économique* ».

23. CJCE, 23 avril 1991, aff. C-41/90, *Klaus Höfner et Fritz Elser c/ Macrotron GmbH* : Rec. CJCE 1991, I, p. 1979. – TPICE, 22 oct. 1997, aff. jtes T-213/95 et T-18/96, *Stichting Certifcatie Kraanverhuurbedrijf (SCK) et Federatie van Nederlandse Kraanverhuurbedrijven (FNK) c/ Commission* : Rec. CJCE 1997, II, p. 1739

24. Cette même CJCE rappelle que « *la notion d'entreprise au sens des dispositions du traité en matière de concurrence n'exige pas que l'unité économique concernée soit dotée de la personnalité juridique* » : CJCE, 28 juin 2005, aff. C-189/02 P, *Dansk Rorindustri A/S*).

25. A. Debet, Des précisions sur le cadre juridique des contrôles et des sanctions prononcées par la CNIL, CCC n° 2, février 2016, comm. 16, à propos de CE 18 novembre 2015, n° 371196, *Société PS Consulting c/ Premier Ministre* : Juris-Data n° 2015-025811 et CE, 18 déc. 2015, n° 384794, *SARL Loc Car Dream c/ CNIL* : Juris-Data n° 2015-028636.

26. Comme cela est le cas pour l'ACPR et l'AMF.

27. Art. 4.8 du RGPD reprenant définition du sous-traitant de la Directive 95/46/CE : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement* ».

28. Art. 10 q et r.

29. Art.28.3 du RGPD.

30. Art.28.3 g du RGPD.

31. Art. 6-1f du RGPD. Un traitement est également légitime s'il procède du consentement au traitement par la personne concernée, de nécessités issues de l'exécution d'un contrat ou de mesures précontractuelles, du respect d'une obligation légale, de la sauvegarde d'intérêts vitaux, de l'exécution d'une mission d'intérêt public et enfin de la nécessité liée aux intérêts légitimes du responsable de traitement ou d'un tiers.

32. Considérant 47 du RGPD.

33. Ibid.

34. WP29 - Opinion 03/2013 on purpose limitation, 2 avril 2013.

35. A savoir de la collecte en vue de finalités spécifiées, explicites et légitimes jusqu'aux

du traitement est une préoccupation majeure en matière de profilage (cf. *infra*). Le respect des principes relatifs à la licéité des traitements fait l'objet d'une amende administrative[36].

7. Sécurité des données personnelles

L'on sait que la loi informatique et libertés prévoit d'ores et déjà une obligation particulière de vigilance s'agissant de la protection des données à caractère personnelle[37]. Outre ce devoir de vigilance, l'article 34 bis II de cette loi prévoit, en cas de violation de données à caractère personnelle[38], une information sans délai de la CNIL[39]. Les articles 32 et 33 du RGPD abordent ce sujet[40].

L'article 32 du RGPD ne déroge pas à cette obligation et prévoit que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque[41]. Par ailleurs, le texte évoque l'évaluation du niveau de sécurité approprié, compte tenu notamment des risques que présente le traitement, en cas de destruction, perte, altération ou divulgation non autorisée de données à caractère personnel.

L'article 33 est consacré à l'obligation de notifier les failles de sécurité, obligation jusque-là réservée aux seuls opérateurs de télécom et qui se trouve généralisée à l'ensemble des responsables de traitements. Le RGPD énonce que les responsables du traitement doivent informer l'autorité de contrôle dans les meilleurs délais et, si possible, « *72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* ». Cette information est accompagnée de la nature de la violation, des catégories de données et du nombre de personnes concernées ainsi que des mesures prises pour atténuer la gravité de la violation. Si l'entreprise prouve qu'elle a mis en place un dispositif de sécurité raisonnable, elle pourra échapper à la notification auprès des personnes concernées, c'est-à-dire ses clients et prospects[42].

Point d'attention

Outre le RGPD, on notera que l'article L. 1332-6-2 du Code de la défense exige des opérateurs d'importance vitale qu'ils informent sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité de leurs systèmes d'information[43]. Sont concernés par cette obligation les opérateurs d'importance vitale[44] exerçant des activités comprises dans un secteur d'activités d'importance vitale[45]. La sécurité des données personnelles est un enjeu majeur face à la montée en puissance des diverses formes de cybercriminalité.

II. DROITS ET OBLIGATIONS RENFORCÉS OU NOUVEAUX

Les articles 12 à 22 du RGPD traitent de sujets clés[46] et font l'objet d'une protection par des amendes administratives très dissuasives[47].

1. Renforcement des droits existants

1.1. Information : de nouvelles obligations d'information sont définies, que les données soient collectées directement auprès de la personne concernée ou indirectement. L'article 13[48] du RGPD dresse la liste les informations devant être communiquées lorsque des données à caractère personnel sont directement collectées auprès de la personne concernée, en y ajoutant celles nécessaires à la garantie d'un traitement équitable et transparent.

Point d'attention

Le responsable du traitement doit veiller à ce que la communication à destination de la clientèle, indépendamment du support employé, soit « *concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* »[49]. Par ailleurs, se posera la question de l'administration de la preuve de la bonne exécution de ces obligations. Les informations peuvent être communiquées oralement si la personne concernée en fait la demande, et à condition que l'identité de cette dernière soit démontrée par d'autres moyens[50].

traitements ultérieurs compatibles avec les finalités exprimées en amont.

36. Amendes administratives pouvant s'élever jusqu'à 20 000 000 euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

37. L'article 34 de cette loi prévoit à cet effet que le « *responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

38. Art. 34 *bis* I : « *[…] on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques* ».

39. La violation de l'obligation de notification d'une violation de données à caractère personnel auprès de la CNIL ou auprès de l'intéressé est punie de cinq ans d'emprisonnement et de 300 000 euros d'amende.

40. La violation de ces dispositions peut donner lieu à des amendes administratives d'un montant maximum de 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

41. A cet égard, le texte vise la pseudonymisation et le chiffrement des données à caractère personnel.

42. La sanction en cas de manquement à ces obligations est prévue par l'article

43. Un décret n° 2016-66 du 29 janvier 2016 (JO du 30 janvier 2016) a institué au ministère de l'économie, en lieu et place du délégué interministériel à l'intelligence économique, un commissaire à l'information stratégique et à la sécurité économiques, chargé d'élaborer et de proposer la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation.

44. Article R1332-1 du Code de la défense.

45. Article R1332-2 du Code de la défense, activités ayant trait à la production et la distribution de biens ou de services au fonctionnement de l'économie.

46. Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée (art 12), informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée (art. 13), informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (art. 14), droit d'accès (art. 15), droit de rectification (art. 16), droit d'effacement -droit à l'oubli (art. 17), limitation du traitement (art. 18), notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement (art 19), portabilité des données (art. 20), droit d'opposition (art. 21) et décision individuelle, y compris le profilage (art. 22).

47. Art. 83-5 du RGPD : amende administrative pouvant s'élever 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

48. L'article 14 du RGPD traite des informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée.

49. Art. 12 du RGPD. Cf. Cf. également les considérants 39, 58 à 63 du RGPD.

50. Ibid.

Article 13[1] : Informations à fournir lorsque les données sont collectées auprès de la personne concernée	Article 14[2] : Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée[3]
Identité du Responsable de Traitement	Idem
Données de contact du responsable du traitement et du DPD	Idem
Finalité du traitement + base légale	Idem
Durée de conservation	Idem
Intérêt légitime poursuivi parle responsable du traitement	Idem
Destinataires ou catégories de destinataires	Idem
Transfert hors UE avec le type de garantie (Clauses contractuelles type[4] et binding corporate rules[5]) et obtention d'une copie de ces garanties	Idem
Durée de conservation des données ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée	Idem
Droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement[6] relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données.	Idem
En cas de consentement donné pour plusieurs finalités y compris des données sensibles[7], mention de l'existence du droit de retirer son consentement à tout moment.	Idem
Droit d'introduire une réclamation auprès d'une autorité de contrôle.	Idem
Informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les informations et les conséquences d'un refus.	
Existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.	Idem
En cas de traitement ultérieur pour une finalité différente communication préalable à la personne concernée des informations au sujet de cette autre finalité.	Idem
	Catégories de données à caractère personnel concernées.
	La source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public[8].

1. Cf. art 32 I à II de la loi informatique et libertés.
2. Cf. art 32 III à VI de la loi informatique et libertés
3. Sous réserve des exceptions limitativement énumérées à l'article 14-5 du RGPD.
4. Ce sont des modèles de clauses adoptés par la Commission européenne permettant d'encadrer les transferts de données personnelles hors de l'Union européenne.
5. Les BCR ou Binding Corporate Rules sont un code de conduite déterminant la politique, au sein d'une entreprise ou d'un même groupe, en matière de traitement de données à caractère personnel. Lorsqu'une CNIL européenne considère que des BCR apportent un niveau de protection suffisant, les autres autorités, par réciprocité, les approuvent automatiquement.
6. Il s'agit du marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur. C'est un statut hybride de la donnée personnelle.
7. Cf. art. 9-2 a du RGPD.
8. Ceci exige une traçabilité complète des données.

1.2. Consentement. Le RGPD n'innove pas en rappelant dans son article 6.1[51] le principe selon lequel le consentement est partie intégrante de la licéité d'un traitement. Ce consentement est défini à l'article 4-11 du Règlement comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair que les données à caractère personnel la concernant fassent l'objet d'un traitement* ».

Non seulement le RGPD apporte des précisions sur les moyens à mettre en œuvre[52] pour assurer la collecte du consentement mais encore, il apporte des précisions[53] relatives aux obligations du responsable de traitement. Ainsi le consentement globalement donné à des conditions générales ne vaut pas consentement au sens du RGPD[54]. Quant au retrait du consentement, il doit être aussi aisé que l'a été son octroi.

Point d'attention

Le consentement pourra être donné « *par un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique,*

51. « *Le traitement n'est licite que si et dans la mesure où la personne concernée a consenti au traitement de ses données à caractère personnel, pour une ou plusieurs finalités spécifiques* ».
52. Recours à la case à cocher lors de la consultation d'un site Internet, paramétrage technique des outils permettant d'utiliser les « *services de la société de de l'information* » (comprendre « *pour naviguer sur Internet en choisissant à qui et pour quelle finalité l'on accepte que ses données soient collectées* »). Cf. considérant 32.
53. Art. 7 du RGPD.
54. Art. 7-2 du RGPD : la demande de consentement ne peut être fondue dans « *une déclaration écrite qui concerne également d'autres questions* ».

éclairée et univoque son accord au traitement des données à caractère personnel la concernant, par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale » [55]**. Se posera, encore une fois, la question de la preuve du consentement communiqué oralement.**

S'agissant des mineurs, l'article 8 du RGPD prévoit que les moins de 16 ans doivent obtenir l'autorisation du titulaire de l'autorité parentale [56] afin de souscrire une offre « *[…] directe de services de la société de l'information* ». Les médias sociaux sont principalement visés mais, de manière générale, la vigilance est de rigueur.

1.3. Profilage. L'article 4-4 du RGPD donne une définition du profilage [57] qui est une notion absolument centrale dans tous les développements liés au numérique et, tout spécialement, s'agissant du recours à des traitements de type big data [58]. Si l'article 22-1 évoque « *[…] le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* ». Ce principe connaît des exceptions, notamment lorsque la décision est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement (art. 22-a).

Les lignes de force en la matière sont les suivantes :

– tout d'abord, nous l'avons vu, les finalités doivent être fixées de manière « *[…] explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités […]* » (art. 5-b du RGPD) ;

– les données doivent être collectées avec discernement, elles doivent êtres « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » (art. 5-c du RGPD). Ce principe est celui de la minimisation des données ;

– un traitement dans un but différent du but originel est possible mais avec précautions [59] ;

– information au sujet de « *la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée* » (Article 13-2 F du RGPD) ;

– possibilité d'opposition au profilage [60] ;

– information sur l'opposition telle que prévue par l'article 13-2 b du RGPD. Il n'y a plus de nécessité, pour la personne concernée, d'invoquer un intérêt légitime.

Point d'attention

L'article 22-3 du RGPD énonce que le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, « *au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement* ». On soulignera qu'une information à ce sujet ne figure pas au nombre de celles mentionnées par l'article 13.

2. Nouveaux droits et obligations

2.1. Droit à l'effacement. À sa demande, la personne concernée peut demander l'effacement des données la concernant, à charge pour le responsable de traitement d'informer les tiers, auxquels il aurait transmis ces données, d'une telle demande. Ce droit n'est pas nouveau mais se voit reconnaître une existence légale (Article 17 du RGPD reconnaissant un « *droit à l'effacement (droit à l'oubli)* »). Ce droit est limité aux cas limitativement énumérés par l'article 17-1.

2.2. Droit à la portabilité. C'est le droit pour la personne d'obtenir une copie de ses données sous forme informatisée et standardisée. La portabilité des données concerne aussi le transfert des données d'un prestataire de services à un autre [61]. L'article 20 du règlement pose trois conditions au droit à la portabilité.

Ce droit doit s'exercer à propos de « *données à caractère personnel* », lesquelles doivent avoir été « *fournies* » par la personne concernée et enfin, le traitement automatisé repose soit sur le consentement des personnes, soit sur l'exécution d'un contrat conclu avec la personne concernée. En matière bancaire, cette portabilité emportera levée du secret bancaire au profit de l'établissement d'accueil, la preuve de cette levée devant être dûment documentée et archivée.

Point d'attention

La portabilité se limite aux informations communiquées par la personne concernée, à l'exclusion des documents issus du responsable du traitement. En bonne logique, elle devrait en outre être limitée de manières diverses. D'une part le transfert ne devrait concerner que les données dont le transfert est pertinent, notamment en fonction de l'obsolescence éventuelle des données concernées (ex. les informations communiquées 20 ans auparavant pour l'instruction d'une demande de crédit). Des lignes directrices sur ce point sont nécessaires, eu égard à son impact opérationnel. Enfin, se posera la question de l'interopérabilité des systèmes d'information et, par voie de conséquence, de l'adoption d'un format unique [62]**. Les services de coffre-fort électronique devraient notamment être concernés par la portabilité.**

2.3. Obligation de nommer un délégué à la protection des données (DPD) [63]. Le RGPD rend obligatoire la dési-

55. Considérant 32 et art 12 du RGPD.

56. Art. 8.2 : « *Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans* ».

57. « *Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».

58. E. Jouffin et X. Lemarteleur, « Du psautier de Mayence au zetaoctets – quel environnement juridique pour le big data ? », *Banque et Droit* n° 166, mars-avril 2016, p. 12.

59. Avis du G 29 : WP29 - *Opinion 03/2013 on purpose limitation*, 2 avril 2013. La relation entre les buts pour lesquels les données personnelles ont été recueillies et les finalités des réutilisations ultérieures, le contexte dans lequel les données personnelles ont été collectées et les attentes raisonnables des personnes concernées quant à leur utilisation ultérieure, la nature des données personnelles et de l'impact de leur utilisation ultérieure, les garanties relatives à un traitement équitable et afin d'éviter tout impact excessif sur les personnes concernées.

60. Art. 21-2 du RGPD : « *Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection* » et considérant 70.

61. Art. 20 du RGPD.

62. On pense à l'Echange de Données Informatisé (EDI) appelé en anglais Electronic Data Interchange, permettant des messages standardisés, de machine à machine, sans intervention manuelle. Les standards ont été fixés au cours des années quatre-vingt.

63. Nommé DPO (*Data Privacy Officer*) dans la version anglaise du RGPD.

gnation d'un DPO pour trois catégories d'entités dont les organismes dont l'activité de base implique un suivi régulier systématique et à grande échelle[64] de personnes ce qui est notamment le cas des établissements du secteur bancaire (établissements de crédit, de paiement et de monnaie électronique)[65]. Un groupe d'entreprises peut nommer un DPD unique[66].

Qui ? Le DPD peut être un membre du personnel du responsable de traitement ou du sous-traitant[67], il peut aussi être externe et être lié par un contrat de prestation de services. Il peut ne pas être exclusivement dédié à l'activité de protection des données et peut assumer d'autres fonctions sous réserve de l'absence de conflits d'intérêts[68]. Le RGPD n'entre pas dans le détail des compétences requises pour être désigné DPD se bornant à énoncer qu'il « *est 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, et de sa capacité à accomplir les missions visées à l'article 39* »[69].

Quel positionnement ? L'article 38-3 est clair « *le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant* » et, à ce titre, le responsable de traitement doit veiller à son indépendance et lui fournir les moyens nécessaires à l'exécution de ses missions[70]. Par rapport au CIL, le DPD est obligatoire, rattaché au plus haut niveau hiérarchique, détenteur d'une expertise attestée et soumis au secret professionnel.

Quelles missions ? Le RGPD attribue plusieurs missions[71] au DPD, dont notamment celles de conseil et de contrôle, mais aussi de relais avec l'autorité de contrôle. On mentionnera principalement le fait d'informer et de conseiller le responsable du traitement ainsi que les salariés traitant des données à caractère personnel sur les obligations qui leur incombent, contrôler la conformité des traitements avec le RGPD et s'assurer de la conservation des documents relatifs à son activité de conseil vis-à-vis du responsable de traitement.

Point d'attention

Le DPD doit être indépendant, ne recevant aucune instruction en ce qui concerne l'exercice de ses missions (art. 38-3). Si le RGPD ne détaille pas moyens dont le DPD doit bénéficier, il est évident que ces derniers devront être proportionnés à l'ampleur de ses missions et se posera la question de sa dotation en effectifs. Il n'est guère douteux que les autorités de contrôle auront leur mot à dire en ce qui concerne ce sujet. La violation des dispositions du RGPD relatives au DPD est objet de sanctions administratives[72], sans préjudice d'autres sanctions que pourrait notamment prononcer le superviseur bancaire.

III. EN ATTENDANT LE 25 MAI 2018…

Il faut, dès à présent, anticiper l'arrivée du RGPD, lequel va impliquer trois chantiers principaux.

1. Audit des processus existants

La prise en compte des nouvelles obligations, notamment en matière d'information, emporte l'obligation d'analyser les processus existants en matière de protection des données et de mesurer les écarts entre l'existant et la cible. Cet audit doit être effectué dans chacun des pays d'implantation au sein de l'UE.

2. Modification des organisations

Le RGPD conduit à un renforcement de la gouvernance des données à caractère personnel et donc, des processus d'élaboration des offres de produits et services. La prise en considération de l'*accountability* doit être une partie intégrante des travaux conduits dans les comités d'examen des produits.

3. Modification des systèmes d'information

Les nouvelles obligations issues du RGPD auront un impact direct sur les systèmes d'informations.

La mise en œuvre du RGPD devra être précédée des réflexions suivantes :

- mesure des coûts actuels de la protection des données et budgétisation des évolutions ;
- évaluer l'impact des différentes mesures induites par le RGPD sur l'existant, y compris les questions de sécurité ;
- évaluer les options possibles en ayant présent à l'esprit que, même s'il est un règlement, le RGPD permet de nombreuses possibilités d'adaptation aux États membres. L'examen des discrétions nationales envisageables doit être rapidement conduit ;
- hiérarchiser les programmes d'actions de mise en conformité ;
- mettre en œuvre et piloter les projets ;
- sensibiliser et former les acteurs internes. ■

64. La notion de « grande échelle » devra être précisée.
65. Art. 37-1 b du RGPD.
66. La notion de groupe d'entreprises est définie à l'art.4-19 du Règlement comme une entreprise qui exerce le contrôle et les entreprises qu'elle contrôle.
67. Art.37-6 du Règlement.
68. Art.38-6 du Règlement.
69. Art. 37-5 du RGPD.
70. Art. 38-2 du RGPD.
71. Art.58 -1,2 et 3 du Règlement.
72. Art. 83-4 du RGPD.