Boond Manager

ET le

By 3X consultants

A. Périmètre de la démarche

Dans le cadre de ses activités et de sa mise en conformité, BoondManager respecte l'ensemble des textes relatifs à la protection des données à caractère personnel, notamment :

- Le traité n°108 du 28 janvier 1981 ;
- La directive « vie privée et communications électroniques » du 12 juillet 2002 ;
- Le Règlement Général relatif à la Protection des Données à caractère personnel (RGPD) du 27 avril 2016 ;
- La loi n° 2016-1321 « pour une République Numérique » (LRN) du 7 octobre 2016 ;
- La loi n°78-17 « Informatique et Libertés » du 6 janvier 1978 modifiée (dernière version adoptée en février 2018).

BoondManager est également attentive aux textes en cours d'étude ou d'adoption, notamment au projet de règlement ePrivacy.

Par ailleurs BoondManager tient compte des recommandations du G29[1], en particulier les recommandations suivantes :

- Lignes directrices concernant sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE adoptées le 9 avril 2014 ;
- Lignes directrices concernant les délégués à la protection des données (DPD) adoptées le 13 décembre 2016 & Version révisée adoptée le 5 avril 2017 ;
- Lignes directrices relatives au droit à la portabilité des données adoptées le 13 décembre 2016 & Version révisée adoptée le 5 avril 2017 ;
- Lignes directrices concernant les données au travail adoptées le 8 juin 2017 ;
- Lignes directrices concernant le profilage et les décisions automatisées adoptées le 3 octobre 2017 et révisées le 13 février 2018 ;
- Lignes directrices concernant les violations de données et leur notification adoptées le 3 octobre 2017 et révisées le 13 février 2018 ;
- Lignes directrices concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du RGPD adoptées le 4 avril 2017 & Version révisée adoptée le 4 octobre 2017 ;
- Lignes directrices concernant le consentement adoptées le 28 novembre 2017 et révisées le 16 avril 2018 ;
- Lignes directrices concernant la transparence des traitements adoptées le 12 décembre 2017 et révisées le 13 avril 2018.

B. Nos mesures organisationnelles

[1] L'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales. Il est appelé « G29 » pour « Groupe de l'article 29 » (ou « Working Party 29 (WP29) » en anglais).

i. Sensibilisation

Il a été procédé, avec l'aide de notre cabinet de conseil externe, à la sensibilisation de l'ensemble du personnel conformément à l'article 39 du RGPD.

ii. Documentation interne

Dans le respect des principes d' « accountability » et « privacy by design » (considérants 78, 85, 108 et articles 3, 25 et 85), BoondManager fait évoluer l'ensemble de ses outils et procédures internes, notamment :

- Procédure de gestion de projets afin d'assurer le respect, pour chaque nouveau projet BoondManager, des principes d'accountability et privacy by design ;
- Charte de protection des données à destination des collaborateurs BoondManager afin d'assoir les règles de confidentialité et sécurité à observer quant au traitement de données à caractère personnel ;
- Politique de protection des données à destination des clients et utilisateurs des produits/services BoondManager afin de respecter le principe de transparence (considérants 39, 58, 78, article 5 et section 1 du RGPD). Cette politique est disponible sur notre site internet *(rubrique « Confidentialité » présente dans le pied de page)* ;
- Politique de gestion des cookies.

iii. Documentation externe

Afin de respecter les exigences évoquées ci-dessus, BoondManager fait également évoluer l'ensemble de ses outils et procédures en lien avec les responsables de traitements, les sous-traitants ou les personnes concernées. Cela concerne principalement les éléments suivants.

a. Consentement des personnes (opt-in)

Nous avons diligenté une étude approfondie sur le consentement afin de nous assurer que nos pratiques et celles que nos Clients peuvent avoir grâce à BoondManager sont en phase avec les exigences du RGPD, le consentement étant la principale base légale utilisée dans les activités de recrutement notamment. Nous déployons actuellement des actions et fonctionnalités en vue du respect des exigences suivantes :

Légende		
=	+	-
Signifie qu'il n'y a pas d'évolution ou que les conséquences des évolutions sont minimes quant à l'utilisation du consentement comme base légale de traitement.	Signifie qu'il y a des évolutions rendant plus aisée l'utilisation du consentement comme base légale de traitement.	Signifie qu'il y a des évolutions nécessitant des actions complémentaires pour l'utilisation du consentement comme base légale de traitement.

Assertions	Directive 95/46/CE	Règlement 2016/679	Evolutions
Validité du consentement Le consentement doit respecter certaines exigences afin d'être valable.	**Article 2h) et 7a)** Manifestation de volonté, libre, spécifique, informée et indubitable.	**Considérant 32 et articles 4-11, 6-1a) et 7** Acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord.	- Le consentement exige une action positive claire de la personne concernée. Cela remet en cause certains cas dans lesquels un consentement pouvait être valable auparavant. « Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».
Consentement « donné librement » Le consentement doit refléter un véritable choix de la personne concernée, effectué en toute liberté. En cas de pression ou contrainte sur la personne concernée, le consentement donné pourra être remis en cause.	**Article 2h)** La directive 95/46 prévoit bien que « le consentement doit être librement donné », mais ne précise pas le sens de cette exigence.	**Considérants 32 et 43 et article 7-4** Si quelque chose souhaité par la personne concernée (produit/service) est subordonné au consentement, ce dernier pourra parfois être remis en cause. Il en va de même si le refus ou retrait du consentement fait peser sur la personne concernée des effets négatifs, ou s'il y a un déséquilibre entre le responsable de traitement et la personne concernée.	- Tandis que la directive de 1995 ne fournit presque aucun renseignement sur la notion de « consentement libre »*, les définitions du RGPD rendent la démonstration d'un consentement valable plus difficile dans certains cas : particulier VS administration, employé VS patron, etc. Dans certaines hypothèses, le recours au consentement doit être tout bonnement écarté. BoondManager n'est pas concernée par cet état de fait. *Avant l'entrée en vigueur du RGPD en 2016 le G29 avait commencé à clarifier la notion, notamment dans son avis 15/2011. Toutefois, bien que très importantes, les recommandations du G29 ne sont pas juridiquement contraignantes.

Consentement « spécifique » Un consentement ne spécifiant pas le traitement pour lequel il est donné n'est pas valable.	**Article 2h)** « La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs **finalités spécifiques** ».	**Considérant 32 et article 6-1a)**	= Comme le G29 a pu le préciser dans son avis 15/2011 précité, le consentement doit être intelligible. La demande de consentement formulée par le responsable de traitement doit clairement et précisément en exposer la portée et les conséquences à la personne concernée. Le consentement ne peut s'appliquer que dans un contexte spécifique, il ne peut être donné de manière indéfinie et illimitée.
Consentement « informé » Afin qu'un consentement soit donné valablement, la personne concernée doit disposer d'informations suffisantes pour lui permettre de comprendre ce à quoi elle va consentir.	**Considérant 25 et article 2h)** La directive de 1995 ne définit pas précisément ce terme.	**Considérants 32 et 42 et articles 4-11 et 7-1** Le traitement objet du consentement doit être décrit à l'aide d'informations « aisément accessibles et formulées en des termes clairs et simples ». « La personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel ».	- Le RGPD implique une plus grande attention dans la rédaction des demandes de consentement.

Le silence ne vaut pas consentement Si ce n'est pas clairement « oui », c'est « non ».	**/** La directive 95/46/CE ne précise rien à ce sujet.	**Considérant 32** « Il ne saurait dès lors y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité ».	- Si la directive ne dit rien, le RGPD reprend et donne quant à lui force juridique aux recommandations du G29 (cf. avis 15/2011 précité). La plupart des demandes de consentements par cases à décocher ne seront bientôt plus valables.
Consentement distinguable Le consentement ne doit pas être noyé au sein d'autres demandes ou considérations.	**/** La directive 95/46/CE ne précise rien à ce sujet.	**Article 7-2** « Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions ».	- Si la directive ne dit rien, le RGPD reprend et donne quant à lui force juridique aux recommandations du G29 (cf. avis 15/2011 précité). *Exit* sans ambiguïté les consentements noyés au milieu de CGU/CGV.
Le consentement peut être retiré à tout moment Un « non » annule immédiatement le « oui ». Toutefois, ce n'est pas rétroactif.	**/** La directive 95/46/CE ne traite pas spécifiquement ce point.	**Considérant 42, 65 et article 7-3** « La personne concernée a le droit de retirer son consentement à tout moment (…). Il est aussi simple de retirer que de donner son consentement ».	- Bien que la directive ne mentionne pas expressément le droit de retirer un consentement, cette aptitude s'est toujours déduite de la nature même de cette base légale. BoondManager a toujours respecté cette possibilité des personnes concernées de formuler des opt-outs.

Obtention du consentement Aucune méthode n'est imposée par les textes.	**/** La directive ne donne aucune information sur les modalités concrètes d'obtention d'un consentement.	**Considérant 32** « (…) par exemple au moyen d'une déclaration écrite, y compris par voie électronique, ou d'une déclaration orale. Cela pourrait se faire notamment en cochant une case lors de la consultation d'un site internet, en optant pour certains paramètres techniques (…) ».	**+** Le RGPD reconnait spécifiquement la validité des méthodes de recueil du consentement les plus couramment utilisées et affirme que tous les outils et méthodes sont recevables du moment que les critères d'un consentement valable vus précédemment sont pris en compte.
***Quid* des consentements recueillis avant l'application du texte ?** C'est là que ça se gâte...	**/** La directive 95/46/CE ne précise rien à ce sujet.	**Considérant 171** « (…) il n'est pas nécessaire que la personne concernée donne à nouveau son consentement **si la manière dont le consentement a été donné est conforme** [au RGPD] ».	**-** Dans de très nombreux cas, les consentements devront être demandés à nouveau en « mode RGPD ».

Les opt-ins pourront être recueillis et conservés dans BoondManager, nous reviendrons vers vous très prochainement avec des informations complémentaires dans un guide pratique.

b. Droit des personnes concernées

Les droits des personnes concernées (ci-dessous les « droits à la PAAROLE ») relativement aux traitements de données les concernant ont été étendus par les articles 15 à 22 du RGPD (prise en charge plus rapide, exercice facilité et nouveaux droits).

Quand bien même ces droits sont à exercer par les personnes concernées auprès des responsables de traitements BoondManager, en tant que votre sous-traitant, continuera de vous accompagner dans la prise en charge et le traitement de ces demandes.
Pour ce faire nous avons défini strictement la procédure à suivre pour chaque droit susmentionné, dans le respect du fond et de la forme imposés par la réglementation (implication de tous les destinataires concernés par le traitement objet de la demande, respect des délais, constitution d'une base de modèles de réponses, etc.).

c. Flux transfrontaliers de données

Pour la mise en œuvre de ses produits et services, bien que les données soient hébergées en Europe, BoondManager pourrait être amenée à réaliser des transferts de données vers des pays non-membres de l'Espace Économique Européen dont les législations en matière de protection des données à caractère personnel diffèrent de celles de l'Union Européenne. Dans de tels cas BoondManager s'assurera, avant de transférer les données, que les entités extérieures à l'Union européenne et les conditions du transfert offrent un niveau de protection adéquat conformément au règlement 2016/679 (chapitre V du RGPD).

BoondManager, pour la conformité des flux transfrontaliers qu'elle met en œuvre, s'appuiera le cas échéant essentiellement sur les mécanismes de conformité suivants :

- Les décisions d'adéquation de l'article 45 du RGPD ;
- Les clauses contractuelles types de la Commission européennes figurant au c) de l'article 46 du RGPD.

BoondManager informera les personnes concernées et les responsables de traitements des flux transfrontaliers préalablement à leur mise en œuvre (cf. nos mesures juridiques/contractuelles).

d. Notification des violations de données

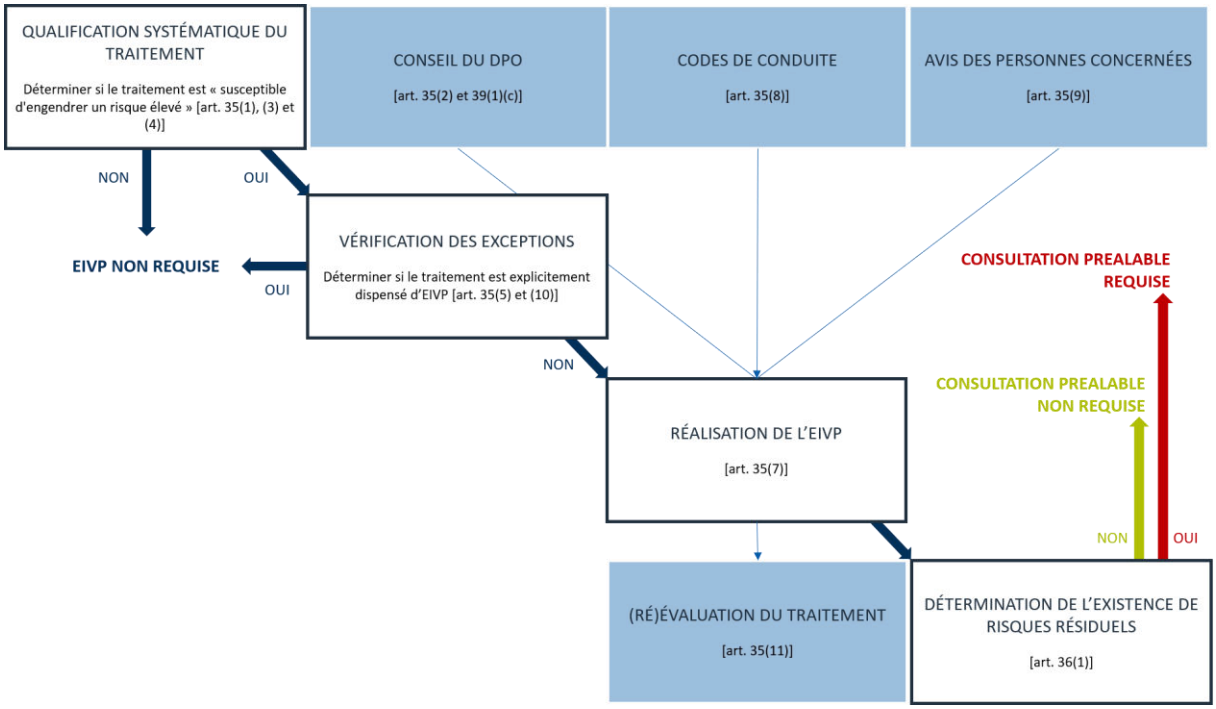
Le RGPD a étendu l'obligation de notification des violations de données à caractère personnel de l'article 34 bis de la loi « Informatique et Libertés » n°78-17 du 6 janvier 1978, jusque-là limitée seuls fournisseurs de services de communications électroniques, à l'ensemble des responsables de traitements et sous-traitants (articles 33 et 34 du RGPD).

De la même manière que pour les droits des personnes, BoondManager a défini la procédure à suivre pour les cas détectés de violations de données dans le respect du fond et de la forme imposés par le RGPD. Cette procédure intègre la réalisation d'une étude d'impact pour chaque violation détectée afin de la qualifier (absence de risque, risque faible à normal, risque élevé) et d'en déduire les règles à suivre (absence de notification, notification de la CNIL et/ou des personnes concernées).

Dans ses procédures, BoondManager prévoit d'informer les responsables de traitements de toute violation de données sans délai afin qu'ils puissent eux-mêmes accomplir leurs formalités dans les 72 heures imparties.

e. Etudes d'impacts sur la vie privée (EIVP)

Conformément à l'article 35 du RGPD, BoondManager a mis en place une procédure relative aux études d'impacts autant pour ses besoins internes que pour accompagner les responsables de traitements dans la réalisation de leurs EIVP. La réalisation des EIVP répond au schéma suivant :



C. Nos mesures opérationnelles

Notre cabinet conseil spécialisé dans la protection des données à caractère personnel a réalisé les audits de nos outils prévus par l'article 39b) du RGPD.

i. Audit des outils

Le plan d'actions a évidemment intégré la réalisation d'audits de BoondManager. Ces audits ont été réalisés sur la base d'un référentiel de complétude réglementaire intégrant les principaux thèmes de conformité RGPD suivants :

- Bases légales,
- Formalités préalables,
- Finalité(s) poursuivie(s),
- Légitimité,
- Qualité des données,
- Destinataires des données,
- Zones de commentaires libres,
- Durées de conservation,
- Interconnexions,
- Flux transfrontaliers,

- Droits des personnes,
- Information des personnes,
- Sécurité/sous-traitance/traçabilité.

ii. Audit des sous-traitants

Le plan d'actions de BoondManager intègre également l'audit de ses sous-traitants, en ce que le RGPD exige une chaine de conformité du responsable de traitement jusqu'au sous-traitant de dernier niveau
BoondManager exige de ses sous-traitants le même niveau de conformité et de rigueur qu'elle s'impose à elle-même.
Tous les sous-traitants qui se révèleront ne pas encore être conformes au RGPD devront prendre un engagement écrit de s'y conformer sans délai. BoondManager s'assurera du respect de cet engagement.

D. Nos mesures juridiques/contractuelles

i. Encadrement de la sous-traitance

Dans le cadre de l'évolution de ses dispositifs de conformité, BoondManager constitue une nouvelle banque de clauses légales relatives à la protection des données pour répondre aux exigences nouvelles du RGPD. Cette banque juridique inclue des clauses relatives à la sous-traitance conformes au RGPD, notamment aux articles 28, 29, 30 et 32 :

- Confidentialité et respect de la réglementation en vigueur ;
- Respect des instructions du responsable de traitement ;
- Description du sort des traitements et des données pendant la durée de la sous-traitance et à son terme ;
- Interdiction de sous-traitance sans accord exprès écrit du responsable de traitement. La demande d'autorisation de sous-traitance emporte communication des informations suivantes :
    - Désignation du sous-traitant ;
    - Nature et volume des traitements sous-traités ;
    - Durée de la sous-traitance ;
    - Lieu et durée de conservation des données par le sous-traitant ;
- Auditabilité du sous-traitant par le responsable de traitement ;
- Report de l'ensemble des engagements de BoondManager sur tout autre sous-traitant autorisé par le responsable de traitement.

Nous allons prévoir ces différentes clauses entre nous et nos sous-traitants. En complément, en tant que votre sous-traitant de confiance, nous avons souhaité nous appliquer lesdites clauses. Vous le retrouverez dans la nouvelle version de notre contrat de service contenant des annexes dédiées à la protection des données à caractère personnel.

ii. Information des personnes

Dans la banque juridique susmentionnée, BoondManager a prévu des clauses légales relatives à l'information des personnes concernées encadrée par les articles 13 et 14 du RGPD. Ces clauses (notamment les clauses conformes à l'article 14 du RGPD) complèteront les informations transmises aux personnes concernées lors de la collecte des données.

Bien que l'information des personnes concernées soit à la charge du responsable de traitement, BoondManager sera force de proposition pour ses Clients et tiendra à leur disposition des clauses conformes RGPD prêtes à personnaliser. Notre guide pratique vous renseignera de façon plus approfondie sur ce point.