
# Comment la mise en œuvre du RGPD par Blackboard va-t-elle aider nos clients ?

Le Règlement général sur la protection des données (RGPD) de l'UE constitue un changement radical. Pour Blackboard, ces changements sont les bienvenus. En effet, nous attachons une grande importance à la protection des données et nous savons que c'est un droit de l'Homme. Le RGPD vient justement réaffirmer les droits des personnes concernées, ce qui nous permettra d'améliorer nos pratiques en matière de protection des données. Cela profitera à la fois aux personnes concernées et aux organisations, en renforçant la confiance qui règne entre tous.

Nous publions ce document pour donner à nos clients un aperçu des changements et des idées reçues entourant le RGPD, présenter notre approche et expliquer dans le détail comment nos efforts peuvent aider votre organisation. Nous nous sommes concentrés sur les informations qui nous paraissent les plus utiles pour vous. Aussi, ce livre blanc n'a pas vocation à être un guide complet sur le RGPD.[1]

Le RGPD apporte des changements considérables, mais Blackboard peut compter sur des pratiques existantes déjà robustes en matière de protection des données (comme notre certification Privacy-Shield UE-États-Unis). Pour nous, le RGPD est une véritable opportunité d'améliorer nos pratiques. Nous continuerons donc de nous concentrer sur nos clients et de vous aider à vous conformer aux lois en matière de protection des données.

*Ces supports ont été élaborés à titre informatif uniquement, et ils ne sauraient constituer un avis juridique. Veuillez demander conseil à vos avocats internes ou externes pour mettre en œuvre le RGPD au sein de votre organisation et pour leur poser vos questions juridiques connexes.*

# TABLE DES MATIÈRES

Blackboard dispose de la certification Privacy Shield (Bouclier de protection de la vie privée) UE-États-Unis, est fier de compter parmi les signataires du Student Privacy Pledge et est membre du Future of Privacy Forum.

# RGPD - CE QU'IL VOUS FAUT SAVOIR

Le RGPD est la nouvelle législation de l'UE en matière de protection des données, qui vient remplacer l'actuelle Directive 96/46/CE sur la protection des données et mettre en œuvre la législation sur la protection des données des États membres de l'UE (comme la Data Protection Act de 1998 au Royaume-Uni).

Le RGPD est entré en vigueur en mai 2016, avec une date butoir de mise en conformité au 25 mai 2018.

Dans les sections suivantes, nous vous donnons un bref aperçu (qui est loin d'être exhaustif) des exigences du RGPD. Vous trouverez également des liens pour obtenir des informations plus détaillées dans la section « Ressources utiles sur le RGPD ».

## Pourquoi cette nouvelle législation ?

Les législateurs et les organismes de réglementation de l'UE étaient convaincus qu'il était nécessaire de mettre à jour la Directive, qui datait de 20 ans, pour faire face au manque d'harmonisation et à l'évolution des technologies et de la société. Parmi les priorités, un renforcement des pouvoirs d'application, un élargissement de la portée territoriale et un renforcement des droits des personnes concernées.

La plupart des nouvelles dispositions (comme l'effet extraterritorial) ciblent principalement les entreprises présentes sur les réseaux sociaux et Internet en dehors de l'UE. Les législateurs et organismes de réglementation de l'UE pensaient que la Directive existante ne protégeait pas suffisamment les droits à la protection des données des ressortissants de l'UE utilisant ces services sur les réseaux sociaux et sur Internet.

Blackboard fonctionne différemment des entreprises ayant adopté, sur les réseaux sociaux et ailleurs sur Internet, un modèle de « monétisation » des données des utilisateurs. Nous collectons et utilisons les informations personnelles[2] de nos clients sur leur ordre et pour pouvoir fournir nos produits et services à nos clients et utilisateurs finaux. Nous ne collectons ni n'utilisons d'informations personnelles dans le but de les vendre ou de vendre de la publicité. Nous comprenons que les informations personnelles nous sont fournies dans le cadre d'une relation de confiance et sont assorties d'obligations. Aussi, nous avons avec nos clients un intérêt et une responsabilité conjoints dans la protection de ces données.

## Qu'est-ce qui change ?

S'il repose sur les principes et concepts de protection des données existant dans l'UE, le RGPD modifie de façon considérable le fonctionnement de la protection des données dans l'UE, et notamment en prévoyant :

- Des amendes pouvant atteindre 4 % du chiffre d'affaires ou 20 millions d'euros (selon le montant le plus élevé)
- Une portée territoriale étendue aux organisations situées en dehors de l'UE fournissant des produits et services à des résidents de l'UE ou contrôlant des résidents de l'UE
- Une obligation de notification des violations aux autorités de contrôle sous 72 heures pour les responsables du traitement[3]
- Des exigences plus strictes en matière de consentement
- Un renforcement des droits des personnes concernées (notamment le droit à l'effacement et à la portabilité des données)

Toutefois, l'un des changements les plus importants concerne les nouveaux principes de responsabilité et de respect de la protection des données dès la conception. Ces principes nécessitent une gouvernance et des processus efficaces de protection des données, ainsi qu'une documentation plus robuste et détaillée de la façon dont chaque organisation se conforme aux exigences du RGPD.

## Qu'est-ce qui ne change pas ?

La plupart des concepts et des définitions du RGPD sont peu ou prou identiques à ceux de la Directive :

- La définition des « informations personnelles » (ou données à caractère personnel/données personnelles) reste pratiquement la même, mais inclut désormais explicitement les adresses IP, les cookies et les identifiants d'appareils
- Les concepts de « responsable du traitement » et de « sous-traitant » restent pratiquement les mêmes (mais le RGPD impose des responsabilités plus directes aux sous-traitants)[4]
- Les principes de traitement définis par la Directive (comme la licéité et l'équité du traitement, la limitation de la finalité, la conservation des informations personnelles uniquement dans la mesure du nécessaire) sont conservés
- Les exigences relatives au transfert des données restent pratiquement les mêmes : les transferts de données en dehors de l'UE/EEE sont autorisés à condition que soit utilisé un mécanisme de transfert de données approuvé (par ex. Privacy-Shield UE-États-Unis ou clauses contractuelles types)[5]

Le durcissement des amendes prévues par le RGPD est là pour rappeler que tout cas de non-conformité avec des principes et exigences existants, comme la conservation des informations personnelles uniquement dans la mesure du nécessaire, ou la mise en place de mesures de sécurité appropriées, est susceptible de présenter un risque accru.

## Quelles sont les conséquences du Brexit ?

Le RGPD sera directement applicable au Royaume-Uni à compter du 25 mai 2018, et jusqu'au « Brexit », fin mars 2019. Cependant, même après le Brexit, le RGPD restera la norme Royaume-Uni :

- En effet, le gouvernement britannique a proposé le UK Data Protection Bill 2017 (projet de loi britannique sur la protection des données, actuellement entre les mains du pouvoir législatif), pour mettre en œuvre le RGPD avant et après le Brexit.[6]
- Après le Brexit, le RGPD s'appliquera directement aux organisations britanniques proposant des biens et des services à des résidents de l'UE ou les contrôlant (comme les universités britanniques recrutant activement des étudiants de l'UE)

Impact sur les transferts de données depuis et vers le Royaume-Uni :

- L'UE a précisé qu'après le Brexit, le Royaume-Uni sera considéré comme un « État tiers », c'est-à-dire qu'il ne sera plus considéré comme un pays « approprié » (sur la liste blanche) pour le transfert des données.
- À moins que le Royaume-Uni soit déclaré approprié par la Commission européenne (par exemple, dans le cadre d'un accord de transition), et jusqu'à ce que ce soit le cas, il faudra mettre en place des contrats et autres mécanismes de transfert des données pour les transferts d'informations personnelles entre l'UE et le Royaume-Uni.
- Inversement, le Royaume-Uni doit déterminer les pays considérés comme appropriés (probablement les États membres de l'UE et les pays sur la liste blanche de l'UE). Pour les pays non considérés comme appropriés, il faudra utiliser des mécanismes de transfert de données reconnus par le Royaume-Uni (probablement similaires aux mécanismes de l'UE) pour transférer des informations personnelles hors du Royaume-Uni.

## Démystifions le RGPD

L'un des objectifs du RGPD est d'apporter davantage de clarté, en définissant des dispositions plus détaillées. Toutefois, de nombreux aspects du RGPD restent ouverts à l'interprétation. De plus, de par sa complexité, le RGPD suscite incompréhension et déclarations exagérées. Cela a donné naissance à des idées reçues et nous en passerons certaines en revue ci-après :[7]

**Idée reçue n° 1 : Le consentement est nécessaire pour tous les traitements d'informations personnelles**

**Fait :** Le consentement n'est que l'une des différentes bases légales du traitement d'informations personnelles (au même titre que, par exemple, les traitements nécessaires à l'exécution d'un contrat ou aux « intérêts légitimes » d'une organisation). Pour le consentement, la barre a été placée très haut. Par exemple, à moins que les personnes concernées puissent consentir librement et révoquer leur consentement à tout moment sans inconvénient, le consentement ne peut être considéré comme valide. Dans la plupart des scénarios de traitement de données, il est préférable d'envisager d'autres bases légales.[8]

**Idée reçue n° 2 : Le délai de 72 heures pour la notification des violations s'applique à l'ensemble de la chaîne logistique (c'est-à-dire à partir du moment où un sous-traitant ou responsable du traitement a connaissance de la violation)**

**Fait :** Le RGPD impose aux sous-traitants de signaler « dans les meilleurs délais » à leur responsable du traitement toute violation d'informations personnelles. Ce n'est qu'une fois que le sous-traitant a informé le responsable du traitement que démarre le délai de notification de 72 heures. Le Groupe de l'Article 29 (G29), qui regroupe les autorités compétentes en matière de protection des données de l'UE, a précisé dans ses lignes directrices finales[9] que « dans les meilleurs délais » implique une notification « rapide » (et pas « immédiate », comme l'avançait un projet précédent).

**Idée reçue n° 3 : Les transferts de données hors de l'UE sont interdits, sauf si le client consent à chaque transfert de données**

**Fait :** De manière générale, le RGPD maintient les exigences actuelles en matière de transfert des données. Ainsi, les transferts de données sont autorisés à condition que soit utilisé un mécanisme de transfert de données approuvé par l'UE, comme le Privacy-Shield UE-États-Unis ou les clauses contractuelles types (contrats de transfert de données). Blackboard a déjà mis en place ces deux mécanismes pour pouvoir transférer de façon conforme les informations personnelles de ses clients.[10]

Comme Blackboard agit en qualité de sous-traitant, le client doit donner des instructions générales pour le transfert des données (contenues dans nos contrats standard de traitement des données), mais il n'est pas nécessaire que le client consente à chaque transfert de données.

**Idée reçue n° 4 : Le droit à l'effacement impose aux organisations d'effacer toutes les données d'une personne concernée**

**Fait :** Le nouveau droit à l'effacement n'est pas un « droit à l'oubli » absolu. C'est plutôt un droit à l'effacement des données si ces dernières ne sont plus nécessaires, et dans d'autres cas, lorsque l'organisation ne respecte pas les exigences du RGPD. Si une organisation a toujours un besoin légitime de conserver des informations personnelles (par exemple du fait d'obligations de conservation de documents), elle n'est pas obligée de les effacer.

**Idée reçue n° 5 : Le RGPD s'applique à toutes les universités ayant des étudiants de l'UE**

**Fait :** Il ne suffit pas d'avoir inscrit des étudiants de l'UE pour que le RGPD s'applique. De manière générale, le RGPD s'applique aux institutions implantées dans l'UE. Il s'applique également aux universités situées hors de l'UE, mais uniquement si elles proposent des biens et services à des ressortissants de l'UE ou contrôlent le comportement de ressortissants de l'UE. Cette « offre de services » suppose un certain niveau de ciblage. La simple inscription d'étudiants de l'UE ne suffit pas. Toutefois, le RGPD peut s'appliquer aux universités qui ciblent activement des ressortissants de l'UE (par exemple, pour des cours en ligne) ou recrutent activement des étudiants dans des États membres de l'UE. Ces critères sont ouverts à l'interprétation et nous recommandons à nos clients de demander un avis juridique.

# MISE EN ŒUVRE DU RGPD

## Pourquoi est-ce important de faire les choses bien concernant la protection des données et les droits du RGPD

La menace de se voir infliger des amendes de 4 % du chiffre d'affaires explique certainement pourquoi de nombreuses organisations ont commencé à prendre plus au sérieux la protection des données. Toutefois, nous estimons qu'il est aussi intéressant de plaider en faveur de bonnes pratiques de protection des données, car la protection des données est un droit de l'Homme et que c'est en adoptant des pratiques robustes de protection des données que nous pourrons créer un climat de confiance.

Dans le monde qui est le nôtre, les informations personnelles sont partout. On dit souvent que c'est le nouveau pétrole de notre économie. Nous utilisons tous des services en ligne et communiquons nos informations personnelles. Mais de nombreuses études démontrent que les personnes ne font pas confiance aux organisations en ce qui concerne les informations personnelles. Le sentiment qui règne est que les personnes ont perdu le contrôle sur leurs données et c'est ce qui a fait réagir les législateurs et organismes de réglementation. Le RGPD en est probablement l'exemple le plus parlant. Les organisations doivent (re)gagner la confiance des personnes, notamment en développant de bonnes pratiques en matière de protection des données. Cela représente également un avantage compétitif. Enfin, cela aidera les organisations à innover. Si les étudiants (et le personnel) ont confiance en votre institution, ils auront plus probablement tendance à fournir leurs données et utiliser de nouveaux outils.

Les conséquences de mauvaises pratiques en matière de protection des données peuvent être catastrophiques et les violations de données font régulièrement la une des journaux. Elles peuvent ternir la réputation d'une entreprise, entraîner une perte de confiance des personnes et donner lieu à des réclamations de la part des personnes dont les données ont été violées. Les autorités de protection des données ne fixeront probablement pas dès le départ des amendes de 4 % du chiffre d'affaires, mais elles disposent de bien d'autres outils d'application et pourront forcer les institutions à faire évoluer leurs pratiques et à mettre en œuvre des programmes de protection des données avec des audits externes réguliers.

## Le rôle de votre organisation et de la nôtre vis-à-vis du RGPD

Le RGPD a conservé les concepts de « responsable du traitement » et de « sous-traitant ». C'est un concept crucial, car il détermine les différentes responsabilités des organisations et de leurs prestataires de services.

Une organisation est considérée comme responsable du traitement si elle détermine les « moyens et les finalités » du traitement des informations personnelles, c'est-à-dire les raisons pour lesquelles et la façon dont les données sont utilisées. En revanche, le sous-traitant est l'organisation qui agit au nom du responsable du traitement et selon ses instructions.

Pour la plupart des produits et services de Blackboard (par ex. Learn, Collaborate, Open LMS), Blackboard est considéré comme le sous-traitant, et nos clients sont les responsables du traitement.

Le RGPD impose davantage d'exigences directes aux sous-traitants comme Blackboard. Cependant, la majorité des exigences du RGPD s'appliquent toujours aux responsables du traitement (par ex. obligation d'informer les personnes sur la façon dont leurs données sont utilisées, de donner suite aux demandes d'accès aux données des personnes concernées, de notifier les violations aux autorités en charge de la protection des données et aux personnes concernées).

## Comment pouvez-vous vous préparer au RGPD ?

Toutes les organisations relevant du RGPD doivent être en conformité au 25 mai 2018. Pour se préparer, nos clients peuvent prendre différentes mesures. Nous avons élaboré cette liste d'étapes d'après notre expérience, et elle n'a pas vocation à être exhaustive. Faites appel à des experts de la protection des données pour vous aider à la mise en œuvre. De nombreuses autorités de protection des données ont également créé des guides pour la mise en œuvre du RGPD.[11]

Normalement, vous devez déjà avoir effectué les étapes 1 à 6 et être en train de mettre en œuvre vos plans d'actions. Mais il n'est jamais trop tard pour commencer. Même si vous venez de vous y mettre, vous pouvez mettre en œuvre les changements les plus importants. Ainsi, vous pourrez également démontrer à votre autorité de protection des données que vous travaillez à un plan d'actions. Vous ne pouvez pas envisager d'ignorer le RGPD.

1. **Vérifier si le RGPD s'applique à votre organisation**

   Si votre organisation est implantée dans l'UE, le RGPD s'applique. Toutefois, il peut également s'appliquer à des organisations implantées hors de l'UE.[12]

2. **Mettre en place un projet de RGPD**

   Concevoir et mettre en œuvre un projet dédié au RGPD. Dans l'idéal, vous devez prévoir une assistance pour les chefs de projet et désigner des interlocuteurs en mesure de vous aider dans chaque service. Ce projet doit couvrir tous les services de votre institution, et vous aurez besoin d'aide.

3. **Désigner un responsable expérimenté pour gérer le projet de RGPD**

   Ce responsable ne doit pas simplement avoir de l'expérience dans la protection des données, il doit également disposer du temps et des ressources suffisantes, ainsi que d'une assistance externe (comme un cabinet juridique). Si votre organisation est une autorité publique implantée dans l'UE, vous devrez également désigner un délégué à la protection des données.

4. **Veiller à l'adhésion et à la supervision des hauts dirigeants**

   Il peut être difficile de mettre en œuvre un projet de RGPD sans l'assistance, l'adhésion et la supervision des hauts dirigeants.

5. **Évaluer votre utilisation des informations personnelles et procéder à une analyse des lacunes**

   La première grande phase de tout projet de RGPD consiste à comprendre où et comment les informations personnelles sont utilisées, et où il est nécessaire de prévoir des améliorations au titre du RGPD.

6. **Élaborer des plans d'actions pour combler les lacunes**

   C'est probablement la partie la plus difficile du RGPD, car elle suppose de traduire les exigences très élevées du RGPD dans des actions spécifiques et concrètes applicables à tous les processus et systèmes.

7. **Mettre en œuvre des plans d'actions**

   La confiance c'est bien, mais dans ce cas, le contrôle, c'est mieux. Cette étape nécessite de contrôler les plans d'actions des autres pour vérifier que chacun respecte ses délais.

8. **Évaluer vos fournisseurs**

   Le RGPD vous tient pour responsable de vos fournisseurs. Il est important de prévoir les bonnes dispositions contractuelles, mais ce n'est pas suffisant. Vous devez également être sûr que vos fournisseurs respectent les exigences du RGPD et peuvent vous aider dans votre démarche de mise en conformité. Demandez-leur également comment ils mettent en œuvre le RGPD.

9. **Rester au fait de l'évolution de la législation et de la réglementation (lignes directrices du Groupe de l'Article 29, lois de mise en œuvre des États membres)**

   Il suffit de connaître le RGPD, pas vrai ? Faux ! Si le RGPD s'applique directement, tous les États membres de l'UE adoptent également des législations nationales complémentaires sur la protection des données.
   Ces législations visent à réglementer les domaines dans lesquels les États membres conservent l'autorité législative (comme la protection des données d'employés) ou dans lesquels le RGPD prévoit un espace de législation complémentaire (comme les critères des délégués à la protection des données et des analyses d'impact sur la protection des données). En outre, le G29 publie des orientations importantes. Il est difficile, mais important, de rester à la page.[13]

# LE PLAN ET L'APPROCHE DE BLACKBOARD

## Protection et sécurité des données chez Blackboard

La sécurité et la protection des données sont des priorités de longue date de Blackboard. Pour nous, le RGPD est une véritable opportunité d'améliorer nos pratiques existantes en matière de protection des données.

Nous avons toujours axé notre approche de la protection des données sur nos clients. Nous comprenons les défis auxquels nos clients sont confrontés et nous voulons les y aider.

Pour avoir de bonnes pratiques en matière de protection des données, il faut un modèle de gouvernance robuste. La protection et la sécurité des données sont l'une des priorités du Conseil de Blackboard et notre modèle de gouvernance (voir ci-dessous) veille à la supervision et à l'accompagnement par les hauts dirigeants de nos efforts en matière de protection et de sécurité des données.

L'importance accordée par Blackboard à la protection et à la sécurité des données se reflète également dans le fait que notre délégué mondial à la protection des données et notre directrice de la sécurité de l'information[14] rendent compte à l'équipe de direction du PDG (voir organigramme ci-dessous)

**Au niveau du Conseil**

### Conseil de Blackboard

- La protection et la sécurité des données sont l'une de ses priorités
- Reçoit des mises à jour régulières sur la gestion des risques de conformité, dont protection et sécurité des données

**Au niveau des hauts dirigeants**

### Comité de conformité

- Supervision pluridisciplinaire des risques de conformité, dont protection et sécurité des données
- Hauts dirigeants, y compris PDG, directeur juridique, directeur financier et responsable de la conformité

### Comité du responsable informatique

- Supervision pluridisciplinaire des risques informatiques et risques liés
- Hauts dirigeants, y compris responsable informatique, responsable de la conformité et membres des équipes de ressources, humaines, finances, service à la clientèle, marketing et produits

**Au niveau des employés**

### Comité de sécurité de Blackboard

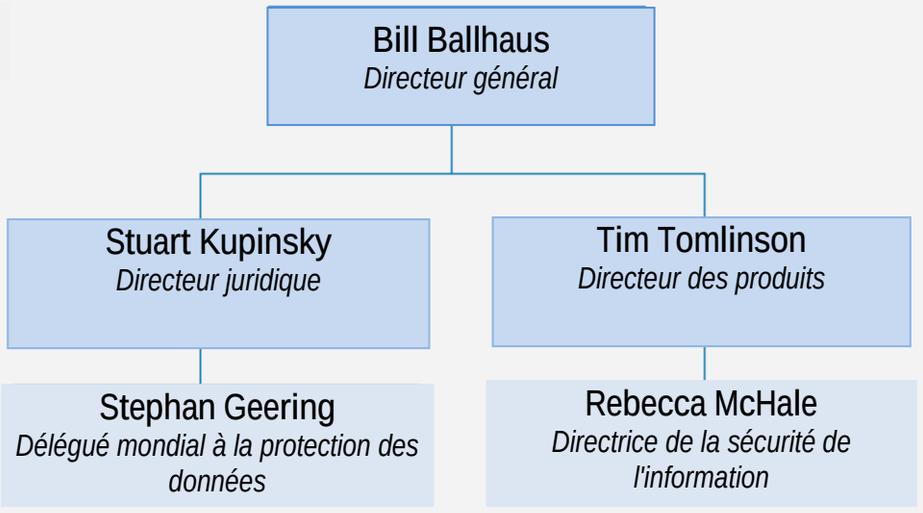
- Supervision de la mise en œuvre en toute sécurité de technologies, politiques et procédures innovantes et efficaces
- Membres : directeur de la sécurité de l'information, chefs de la sécurité des produits, responsable de la conformité, délégué mondial à la protection des données

### Groupe de travail sur le programme de protection des données

- Appui au programme mondial de protection des données/mise en œuvre du RGPD
- Membres : délégué mondial à la protection des données, directeur de la sécurité de l'information, responsable de la conformité, DP, chef de projet, gestion des risques des fournisseurs

Protection des données et sécurité

L'importance accordée par Blackboard à la protection et à la sécurité des données se reflète également dans le fait que notre délégué mondial à la protection des données et notre directrice de la sécurité de l'information rendent compte à l'équipe de direction du PDG.




## L'approche de Blackboard vis-à-vis du RGPD

Nous avons défini un programme complet de mise en œuvre des exigences du RGPD selon l'approche suivante :

- La mise en œuvre du RGPD repose sur l'expérience en matière de protection des données et des mécanismes de conformité déjà en place chez Blackboard
- La mise en œuvre du RGPD est dirigée par le délégué mondial à la protection des données, assisté d'un chef de projet dédié et de responsables du RGPD dans chaque secteur fonctionnel
- Le célèbre cabinet juridique Bristows LLP, entre autres, s'implique dans l'appui à la mise en œuvre du RGPD
- La mise en œuvre du RGPD est supervisée par le Comité de conformité de Blackboard, composé du PDG de l'entreprise, du directeur juridique et d'autres hauts responsables

## Le RGPD, une véritable opportunité

Nous pensons que la mise en œuvre du RGPD ne doit pas être envisagée comme un simple effort de conformité aux nouvelles obligations de l'UE en matière de protection des données, mais surtout comme une opportunité. Aussi, nous comptons mettre à profit la mise en œuvre du RGPD pour accomplir les objectifs suivants :

- Renforcer nos pratiques mondiales de protection des données – nous mettrons à profit le projet de RGPD pour consolider notre programme mondial de protection des données, et pas seulement dans l'UE
- Respecter la protection des données dès la conception, pour intégrer davantage la conformité à nos processus quotidiens
- Accompagner nos clients dans leurs efforts de mise en conformité avec le RGPD
- Imposer Blackboard comme le leader incontesté de la protection des données pour les technologies de l'éducation

## Notre plan de mise en œuvre

Nous avons repris la méthodologie en 3 phases de Bristow LLP pour mettre en œuvre notre programme mondial de protection des données/RGPD. Cette méthode a été reprise par de nombreuses autres entreprises, y compris de grandes entreprises technologiques. Il s'agit des trois phases suivantes :

- **PHASE 1 - Collecte d'informations**
- **PHASE 2 - Élaboration de solutions**
- **PHASE 3 - Mise en œuvre de flux de travail**

Nous avons utilisé cette méthodologie en 3 phases pour élaborer notre programme, qui se décompose en 4 étapes clés :

### Initiation du projet

Étape d'initiation du projet, avec les activités suivantes :

- Information et adhésion des hauts dirigeants
- Embauche d'un délégué mondial à la protection des données, chargé de diriger le projet de RGPD
- Élaboration d'un plan et d'une gouvernance de projet
- Première collecte d'information et évaluation des activités actuelles de conformité pour les domaines à améliorer en vertu du RGPD

### PHASE 1 - Collecte d'informations (ateliers)

Pendant la phase initiale, nous avons organisé des conversations/ateliers structurés avec les principaux acteurs des secteurs fonctionnels et des groupes de produits de Blackboard afin de collecter des informations détaillées sur leurs pratiques de traitement de données.

Nous avons utilisé les résultats des ateliers pour procéder à l'analyse des lacunes et élaborer les solutions et plans de mise en œuvre de la phase 2.

### PHASE 2 - Élaboration de solutions

D'après les résultats des ateliers, nous avons élaboré les solutions et documentations suivantes :

- Documentation améliorée des pratiques internes de protection des données (politique et normes opérationnelles détaillées) reflétant les exigences du RGPD et expliquant comment ces dernières devront être respectées dans le cadre des différentes activités de traitement de données (par ex. exigences de traitement de données de clients, processus de respect de la protection des données dès la conception)
- Exigences de produits
- Plan de mise en œuvre pour les secteurs fonctionnels et les efforts centralisés

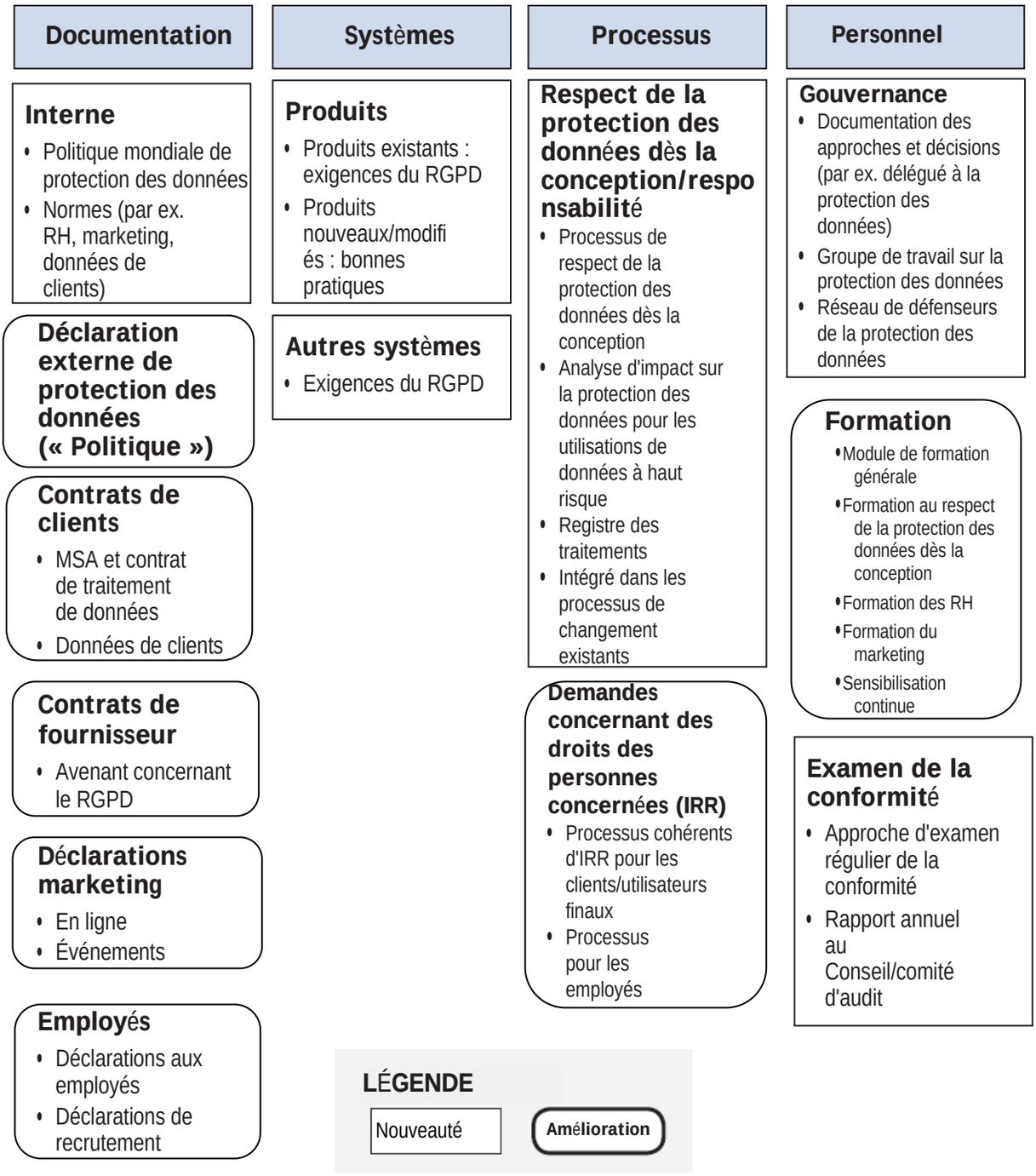
### PHASE 3 - Mise en œuvre de flux de travail

Pendant la phase finale, nous mettons en œuvre le projet de documentation des pratiques de protection des données et les plans de mise en œuvre. Pour ce faire, nous avons mis en place six flux de travail principaux :

1. Exécution des plans de mise en œuvre pour les secteurs fonctionnels et groupes de produits
2. Évaluation et mise à jour des politiques, déclarations et consentements destinés au public
3. Renforcement de la gouvernance (rôles et responsabilités, formation, respect de la protection des données dès la conception, etc.)
4. Évaluation et mise à jour des contrats de fournisseurs (si nécessaire)[15]
5. Modification des systèmes informatiques (si nécessaire)
6. Mise en place d'un registre des traitements de données

## Aperçu des changements

Le graphique suivant explique comment nous envisageons l'état définitif de notre programme de RGPD/protection des données, une fois les activités de mise en œuvre terminées. Une fois le projet de RGPD mis en œuvre, nous continuerons d'innover et de nous adapter pour faire progresser nos pratiques en matière de protection des données.



# COMMENT NOTRE PROGRAMME DE RGPD PEUT-IL VOUS AIDER ?

Le programme mondial de protection des données/mise en œuvre du RGPD de Blackboard vise à aider votre organisation à mettre en œuvre le RGPD. Les sections suivantes détaillent plus avant les 7 points clés suivants :

1. **Des produits compatibles avec le RPGD :** nous mettons en œuvre des exigences de produits pour accompagner nos clients dans leurs besoins de transparence, dans la gestion des demandes concernant les droits des personnes concernées, etc.
2. **Respect des données dès la conception :** nous mettons en œuvre un processus de respect de la protection des données dès la conception et d'analyse des impacts sur la protection des données pour faciliter la documentation de la conformité
3. **Transferts de données :** nous continuerons de mener une approche à plusieurs niveaux : régionalisation, Privacy-Shield UE-États-Unis et clauses contractuelles types approuvées par l'UE
4. **Contrats conclus avec des clients :** nous disposons d'un avenant à notre contrat-cadre standard compatible avec le RGPD pour le traitement des données
5. **Nos fournisseurs :** nous disposons de contrats robustes et d'un cadre de gestion des risques des fournisseurs
6. **Sécurité :** nous avons mis en place une politique, des procédures et une gouvernance améliorées en continu pour préserver la sécurité des données de nos clients
7. **Notification des violations :** nous disposons d'un processus de réaction en cas d'incident de sécurité, documenté et testé

## 1. Des produits compatibles avec le RPGD

Nos flux de mise en œuvre visent principalement à aider nos clients en proposant des produits compatibles avec le RGPD. Pour ce faire, nous avons défini des exigences minimales relatives au RGPD et à la protection des données pour nos produits. Conformément à notre volonté de renforcer nos pratiques mondiales de protection des données, la plupart de ces exigences s'appliquent à tous nos produits, et pas seulement à ceux que nous proposons dans l'UE. Ainsi, nous pourrons également aider nos clients situés hors de l'UE, mais susceptibles de relever du RGPD.

Le développement des exigences appliquées à nos produits en matière de RGPD/protection des données découle d'un processus robuste et intensif. Nous avons d'abord rédigé une version initiale avec un conseiller externe. Ensuite, lors de différentes sessions de travail et révisions organisées avec les principaux acteurs de nos équipes de développement et de gestion de produits, nous avons peaufiné la première version jusqu'à obtenir des exigences générales pour nos produits, qui sont également spécifiques et concrètes, avec des orientations détaillées. Ensuite, les exigences du RGPD et de protection des données de nos produits ont été traduites dans des actions spécifiques aux différents produits et dans des plans de mise en œuvre pour les différents groupes de produits.

Les exigences pour nos produits[16] relèvent des catégories suivantes :

### Transparence

- Possibilité pour les clients de créer un lien avec leurs propres politiques et déclarations de protection des données
- Communication d'informations sur l'utilisation habituelle des informations personnelles en rapport avec un produit

### Minimisation/effacement des données

- Examen des produits pour identifier les champs inutiles/facultatifs
- Examen des produits pour identifier les possibilités de recourir à des données anonymes ou protégées par pseudonyme plutôt que des informations personnelles
- Possibilité d'effacer des informations personnelles sur demande de clients (si les clients/utilisateurs ne peuvent pas les effacer eux-mêmes)

### Droits généraux des personnes concernées

- Capacité à permettre l'accès à et à la rectification des informations personnelles sur demande de la personne concernée
- Capacité à effacer les informations personnelles sur demande de la personne concernée

### Droits des ressortissants de l'UE

- Capacité à traiter les demandes de portabilité des données (droits des personnes concernées à recevoir leurs données dans un format lisible par une machine dans certains cas)
- Possibilité d'arrêter d'utiliser des informations personnelles (droit d'opposition/droit de limitation du traitement dans certains cas)

Blackboard a déjà défini des programmes de sécurité de ses produits tenant compte du RGPD. Par conséquent, nous n'avons pas eu besoin de définir de nouvelles exigences de sécurité spécialement pour le RGPD.[17]

## 2. Respect des données dès la conception

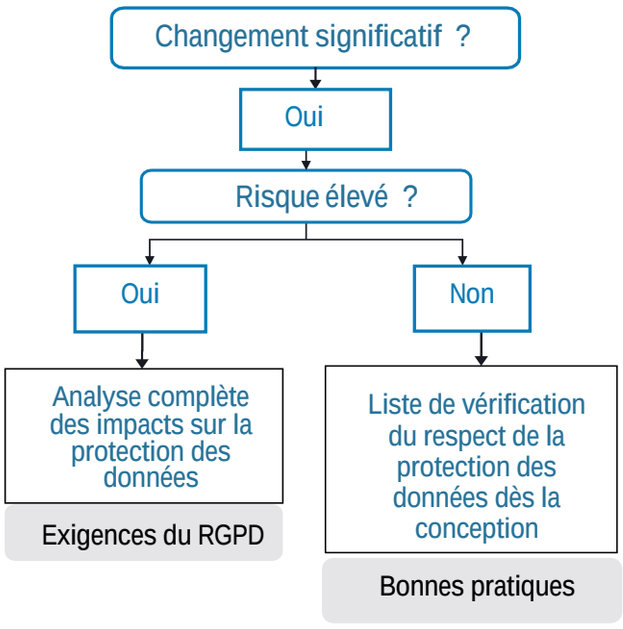
Comme de nos jours, les personnes concernées ont de plus en plus de mal à garder le contrôle sur leurs données (voir notre article de blog sur la protection des données traitant de ce sujet), le respect des données dès la conception et la responsabilité sont de plus en plus importants pour garder la confiance des personnes, des clients et des organisations de réglementation, et pour documenter la façon dont l'organisation applique le RGPD. Nous avons donc placé notre approche du respect des données dès la conception au cœur de notre programme mondial de protection des données/RGPD.

Pour Blackboard, il s'agit plus d'une évolution que d'une révolution. Nous avons toujours procédé à un examen juridique des nouveaux produits et pratiques. Notre approche de respect de la protection des données dès la conception nous permet de formaliser et de mieux documenter ces examens.

### Approche

- Nous avons créé un processus de respect des données dès la conception ainsi qu'une liste de vérification.
- Les processus de changement des secteurs fonctionnels et les groupes de produits incluent le respect des données dès la conception.
- Chaque modification substantielle de l'utilisation d'informations personnelles nécessite de suivre la liste de vérification du respect des données dès la conception. Même si le RGPD ne l'impose pas précisément, c'est une bonne pratique à adopter.
- En effet, cette liste de vérification permet de planifier une analyse plus détaillée des impacts sur la protection des données pour les utilisations à haut risque d'informations personnelles (exigence du RGPD)

Le graphique suivant illustre cette approche :




### 3. Transferts de données

Le RGPD n'impose pas de grands changements sur les modalités de transfert d'informations personnelles en dehors de l'UE/EEE. Les mécanismes et restrictions actuels ont été conservés. Cela signifie que les transferts de données sont autorisés à condition que soit utilisé un mécanisme de transfert de données approuvé par l'UE, comme le Privacy-Shield UE-États-Unis ou les clauses contractuelles types (contrats de transfert de données). Ces mécanismes visent à garantir une protection adéquate des informations personnelles, même en dehors de l'UE/EEE.

Nous maintiendrons donc notre approche redondante et à plusieurs niveaux de la conformité des transferts de données. Cela signifie que nous appliquerons les exigences en matière de transfert de données de différentes façons pour garantir l'existence de mesures adéquates de protection de vos données :

- **Hébergement régional :** nous avons mis en place une stratégie d'hébergement régional, et la plupart de nos produits hébergés dans l'UE, ainsi que d'autres produits, doivent être déplacés vers des solutions d'hébergement régional. Bien que le RGPD n'impose pas le stockage régional des données, et même si nous ne pensons pas que l'emplacement des données puisse jouer sur leur protection ou leur sécurité,[18] nous comprenons que bon nombre de nos clients basés dans l'UE préfèrent que leurs données le soient également.
- **Privacy Shield :** Blackboard a la certification Privacy-Shield UE-États-Unis, ce qui nous permet de transférer légalement des informations personnelles vers les États-Unis.
- **Clauses types :** nous utilisons également des « clauses contractuelles types » approuvées par l'UE et nous permettant de transférer en toute conformité des informations personnelles hors de l'EEE et à destination des différentes entreprises du groupe Blackboard (« contrat de transfert de données de clients »).
- **Fournisseurs :** nous avons mis en place des contrats robustes avec nos fournisseurs et partenaires (par ex., IBM, Amazon Web Services) pour faire en sorte que nos exigences en matière de transfert de données (et autres obligations en matière de protection de données) s'appliquent également à nos fournisseurs et partenaires.

Nous possédons actuellement[19] plusieurs centres de données régionaux prenant en charge le traitement de données dans l'UE et pour nos clients basés dans l'UE :

- Hébergement géré (centres de données de Blackboard) : centres de données à Amsterdam (Pays-Bas) et Francfort (Allemagne).
- Hébergement sur le cloud (centres de données d'AWS) : AWS dans la région de Francfort, Allemagne (centre de l'UE-1).

Les centres de données d'AWS peuvent se prévaloir de différentes certifications et exigences, des normes ISO 27001 et ISO 27018 à SOC2 en passant par la conformité au RGPD et aux exigences locales, comme les lois fédérales allemandes C5 et IT-Grundschutz (protection informatique de base).[20]

Il est important de comprendre que si les informations personnelles de clients sont stockées dans ces centres de données pour la plupart de nos produits (y compris Learn 9.1, Learn SaaS, Open LMS et Collaborate) pour nos clients basés dans l'UE, l'accès à ces données à partir d'un endroit situé hors de l'UE/EEE peut s'avérer nécessaire à la fourniture des produits et services (comme l'assistance 24 h/24-7 j/7). Ces transferts de données sont autorisés grâce à la certification Privacy-Shield UE-États-Unis et aux clauses contractuelles types mentionnées.

## 4. Contrats conclus avec des clients

La Directive actuelle impose aux responsables du traitement de conclure un contrat avec leurs fournisseurs (sous-traitants), mais ne précise pas ce que doit contenir exactement ce contrat. Le RGPD est plus prescriptif et précise une liste de contenus obligatoires.[21]

Notre avenant standard actuel concernant le traitement des données reprend tous les points obligatoires ci-dessous. Il est automatiquement inclus dans notre contrat-cadre standard pour nos clients relevant du RGPD.

✓ Utilisation des informations personnelles uniquement selon les instructions

✓ Signature de contrats de confidentialité par le personnel

✓ Prise de mesures de sécurité appropriées

✓ Recours à des fournisseurs (sous-traitants) uniquement…

- Tel qu'autorisé par le responsable du traitement (il peut s'agir d'une autorisation générale)
- Contraints contractuellement de respecter les mêmes obligations en matière de protection des données

✓ Assistance du responsable du traitement dans la réponse aux personnes concernées faisant valoir leurs droits

✓ Assistance du responsable du traitement vis-à-vis des mesures de sécurité, des notifications de violations et des analyses d'impact sur la protection des données

✓ Restitution ou effacement des données en fin de contrat

✓ Communication des informations nécessaires pour que le responsable du traitement puisse démontrer sa conformité

✓ Information immédiate du responsable du traitement si des instructions du responsable enfreignent le RGPD

## 5. Gestion de nos fournisseurs

Blackboard a recours à des fournisseurs (par ex. IBM, Amazon Web Services) pour proposer ses produits et services à ses clients. Lorsque ces tâches nécessitent un accès à des informations personnelles de nos clients, Blackboard est responsable des pratiques de ses fournisseurs en matière de protection des données.

Dans le cadre de notre programme de RGPD, nous associons étroitement notre approche de respect de la protection des données dès la conception et nos processus actuels de gestion des risques de fournisseurs et d'approvisionnement. En découlent les contrôles clés suivants :

- Des contrats robustes avec un avenant concernant le RGPD et la protection des données pour les tiers, avec des dispositions substantiellement équivalentes à celles que nous avons mises en place avec nos clients
- Des « clauses contractuelles types » et/ou un avenant concernant le RGPD et le Privacy-Shield UE-États-Unis pour permettre de transférer légalement des données à nos fournisseurs
- Une politique et un cadre documentés de gestion des risques des fournisseurs
- Les nouveaux fournisseurs ayant accès aux informations personnelles doivent remplir un Questionnaire d'évaluation de la sécurité du fournisseur, qui comprend des questions concernant la conformité aux principes de protection des données
- Les fournisseurs ayant accès aux systèmes gérés par Blackboard devront respecter les politiques d'autorisation et de contrôle des accès et de l'identité internes de Blackboard, avec des examens de comptes si nécessaire
- Les fournisseurs doivent accéder aux ressources de Blackboard en utilisant des mécanismes approuvés (par ex., VPN)
- Les fournisseurs ont un accès limité pour le contrôle du trafic, des utilisateurs et des actifs

## 6. Sécurité

Le RGPD n'impose pas de changements substantiels au niveau des mesures techniques et opérationnelles de protection des informations personnelles. Ces mesures doivent être « appropriées » en fonction du risque, comme pour la Directive actuelle. Aussi, nous continuerons d'utiliser nos programmes existants de sécurité de l'information.

### Gestion du risque de sécurité des données

Nous avons mis en place une politique, des procédures, une gouvernance et des exigences techniques pour gérer les risques liés à la sécurité informatique pour toutes nos activités.

Dès leur arrivée, les membres du personnel de Blackboard doivent comprendre leurs responsabilités en matière de protection des informations personnelles de nos clients :

- Politique d'identification pour protéger les données sensibles
- Formation annuelle à la sécurité des utilisateurs et à la protection des données
- Exercices de lutte contre le phishing
- Communiqués de sensibilisation

Les exigences suivantes ont été mises en place pour assurer la protection des données par notre personnel :

- Les données sont catégorisées et des exigences ont été définies pour protéger chaque type de données. Les données de nos clients, c'est-à-dire des institutions et de leurs étudiants, sont les plus sensibles.
- Des mesures techniques ont été prises pour protéger les données, par ex. :
  - recours au chiffrement
  - mises à jour de sécurité rapides
  - contrôles d'authentification renforcés
  - protection contre les e-mails malveillants et protection de la navigation sur Internet
  - technologies de protection des terminaux
  - limitation de l'accès aux personnes ayant besoin de connaître les données

### Il n'y a pas que le RGPD...

En tant qu'entreprise mondiale au service de la communauté éducative, nous contrôlons étroitement les lois et réglementations locales applicables en matière de protection et de sécurité des données spécifiques au secteur de l'éducation.

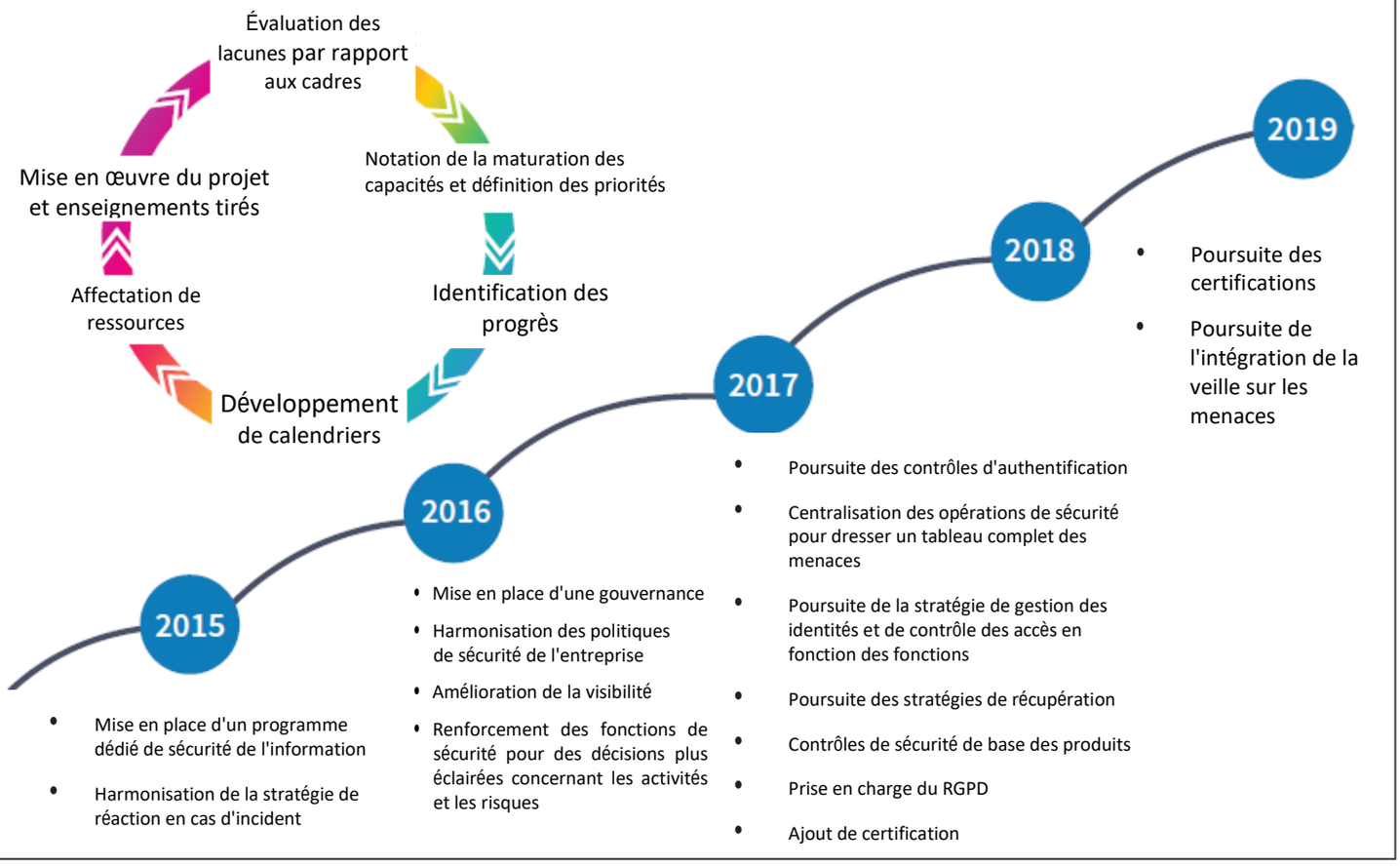
Nous répertorions ci-après quelques exemples de réglementations, normes et cadres applicables à la protection et à la sécurité des données que Blackboard prend en compte, en plus du RGPD, pour élaborer ses politiques, processus et contrôles techniques de sécurité.

- Family Education Right and Privacy Act (FERPA), Protection of Pupil Rights Amendment (PPRA) (États-Unis)
- Children's Online Privacy Protection Act (COPPA) (États-Unis)
- Lois étatiques des États-Unis (mosaïque existante et émergente des 50 États)
- Normes gouvernementales des États-Unis – FedRAMP
- Normes PCI de sécurité des données, si applicable
- ISO/CEI, OWASP, NIST
- Normes internationales (MTCS, IRAP)

### Évaluations de la maturité de la sécurité et feuilles de route

Nous nous efforçons continuellement d'améliorer nos mesures de sécurité opérationnelles et techniques.
Le schéma de la page suivante illustre nos évaluations continues de la maturité et nos feuilles de route.

## Adoption de cadres : évaluations de la maturité de la sécurité et feuilles de route




## 7. Notification des violations

L'un des principaux changements apportés par le RGPD concerne l'obligation de notification des violations d'informations personnelles à l'autorité compétente en matière de protection des données et (dans certains cas) aux personnes touchées.[22] Pour la plupart de nos produits et services, Blackboard agit en qualité de sous-traitant[23] au sens du RGPD. L'obligation de notification aux autorités compétentes en matière de protection des données et aux personnes concernées des violations de données traitées par Blackboard incombe donc à nos clients. Toutefois, le RGPD impose aux sous-traitants comme Blackboard d'informer leurs clients (responsables du traitement) dans les meilleurs délais (c'est-à-dire rapidement)[24] de ces situations.

Nous avons mis en place les mesures suivantes pour aider nos clients à remplir leurs obligations en cas de violation d'informations personnelles traitées par Blackboard pour le compte d'un client :

- Processus de réaction en cas d'incidents de sécurité de Blackboard
  - Documenté et testé régulièrement
  - Permet une identification, une enquête et une résolution rapides des incidents
  - Permet d'informer rapidement les clients
  - Repose sur l'équipe en place de réaction en cas d'incident de sécurité (qui comprend le directeur de la sécurité de l'information et le délégué mondial à la protection des données)
- Notre obligation d'information rapide de nos clients est indiquée expressément dans notre contrat-cadre standard et dans notre avenant concernant la protection des données actuels[25]

# CONCLUSION

Le RGPD impose des changements importants, dont les effets se feront ressentir bien au-delà de la date de mise en conformité, le 25 mai 2018. Nous espérons que ce livre blanc vous aidera à mettre en œuvre le RGPD et a su vous montrer à quel point Blackboard prend le RGPD et la protection des données au sérieux.

Les sections suivantes contiennent d'autres informations utiles ainsi que nos coordonnées, pour tous commentaires ou questions concernant ce livre blanc.

# RESSOURCES UTILES SUR LE RGPD

Les ressources répertoriées ci-après ne constituent qu'un petit échantillon de tous les supports utiles disponibles en ligne. Elles n'ont pas vocation à constituer une liste exhaustive.

Demandez conseil à des experts pour une analyse complète de la mesure dans laquelle le RGPD s'applique à vous. Il est important de faire appel à des experts de la protection des données (comme le cabinet juridique de votre choix).

## Ressources officielles de l'UE

- Texte du RGPD
- Lignes directrices du Groupe de l'Article 29
- Site de la Commission européenne sur le RGPD

## Supports d'autorités de protection des données de l'UE

- Au Royaume-Uni, l'Information Commissioner's Office (ICO) a mis en place un excellent site consacré au RGPD, qui contient des ressources utiles formulées dans un langage clair et est régulièrement mis à jour
- En Irlande, le Data Protection Commissioner (DPC) a dédié une page au RGPD pour les organisations
- En France, la CNIL propose certains supports en anglais, notamment un logiciel gratuit d'analyse d'impact sur la protection des données (ainsi que d'autres documents en français)
- En Espagne, l'AEPD a mis au point un guide à destination des institutions éducatives (PDF, en espagnol)

## Guides de cabinets juridiques

- Guide de Bird & Bird sur le RGPD
- Suivi de la législation des États membres par Bird & Bird (suivi des variations nationales du RGPD)
- Guide de survie au RGPD de Linklaters (PDF)
- Manuel du RGPD de White & Case

## Autres organisations

- JISC UK propose des ressources, des événements et des articles de blog utiles sur le RGPD
- UCISA a publié un document compilant des bonnes pratiques concernant le RGPD, avec des étapes concrètes et des études de cas
- L'Association internationale des professionnels de la protection de la vie privée (IAPP) propose une newsletter hebdomadaire intéressante (et gratuite) sur l'évolution de la protection des données en Europe
- L'IAPP offre également une présentation utile des fournisseurs d'outils de protection des données (PDF)
- Amazon Web Services propose un centre dédié au RGPD

## BIOGRAPHIES

### Stephan Geering

*Délégué mondial à la protection des données*

- Responsable mondial de la conformité aux lois de protection et de sécurité des données
- Dirige le programme mondial de protection des données/mise en œuvre du RGPD
- Rend compte au directeur juridique ; membre de l'équipe juridique de Blackboard
- Basé à Londres

**Le parcours de Stephan :**

- Avocat/commissaire adjoint à la protection des données d'une autorité suisse cantonale de protection des données (2002-2008)
- LLM (Master en droit) au University College de Londres (2008-2009)
- Directeur adjoint en charge de la protection des données du groupe Barclays (2010-2012)
- Directeur de la région EMEA en charge des activités de protection des données de Citigroup (2012-2014)
- Responsable de la protection des données des régions EMEA et APAC de Citigroup (2014-2017)
- Certifié CIPP/E

### Rebecca McHale

*Directrice de la sécurité de l'information*

- Dirige la stratégie de sécurité des produits et infrastructures
- Supervise la gouvernance de la cybersécurité chez Blackboard
- Rend compte au directeur des produits
- Basée à Washington, D.C.

**Le parcours de Rebecca :**

- A rejoint Blackboard en 2016 ; depuis peu, elle dirige à la fois les équipes de sécurité et assure des fonctions importantes pour l'organisation de la sécurité au sein de l'entreprise
- Master en mathématiques discrètes appliquées à l'informatique au Royal Holloway, Université de Londres
- Anciennement directrice des cyberprogrammes de Novetta et CSRA, travaillant pour le gouvernement américain et des clients commerciaux, comme le Département d'État, l'agence nationale américaine de sécurité dans les transports (TSA) et l'agence nationale américaine de garantie des dépôts bancaires (FDIC)

## PLUS D'INFORMATIONS

Vous pouvez trouver plus d'informations sur nos services dédiés à la protection de la vie privée et sur la Page de la communauté de sécurité.

Nous avons également un bulletin d'information sur la protection des données personnelles. Si vous souhaitez recevoir notre bulletin d'information ou si vous avez des questions ou des commentaires au sujet de ce livre blanc, veuillez nous contacter à privacy@blackboard.com.

## Notes

1 Consultez la section « Ressources utiles sur le RGPD » en fin de document pour plus d'informations sur le RGPD.

2 Nous avons choisi d'utiliser le terme « informations personnelles » plutôt que « données à caractère personnel », mais ce terme a la même signification et la même portée que le terme « données à caractère personnel ».

3 Le responsable du traitement est l'entreprise qui détermine les moyens et la finalité du traitement des informations personnelles (les raisons pour lesquelles et la façon dont les données sont utilisées).

4 Voir la section « Le rôle de votre entreprise et de la nôtre vis-à-vis du RGPD ».

5 Voir la section « Démystifions le RGPD » pour plus d'informations sur les transferts de données.

6 Voir le document « An introduction to the Data Protection Bill » de l'ICO pour une présentation utile du projet de loi.

7 Voir également les articles de blog de l'ICO du Royaume-Uni sur les Idées reçues sur le RGPD.

8 Voir également les Lignes directrices du G29 sur le consentement (ébauche) en vertu du Règlement 2016/679 (WP259) et les orientations de l'ICO
sur le consentement.

9 Lignes directrices du G29 sur la notification des violations d'informations personnelles en vertu du Règlement 2016/679 (WP250rev.01).

10 Voir également la section « Transfert des données ».

11 Voir par exemple le document Preparing for the GDPR – 12 steps to take now (PDF) de l'ICO du Royaume-Uni.

12 Voir également la section « Démystifions le RGPD ».

13 Voir la section « Ressources utiles sur le RGPD ».

14 Pour plus d'informations sur le délégué mondial à la protection des données et la directrice de la sécurité de l'information, voir la section « Biographies ».

15 Dans le cadre du projet de certification Privacy-Shield UE-États-Unis, nous avons d'ores et déjà intégré les dispositions contractuelles nécessaires au RGPD à la plupart des contrats conclus avec nos fournisseurs (sous-traitants) ayant accès à des informations personnelles de l'UE.

16 Toutes les exigences ne s'appliquent pas à tous les produits. Par exemple, certains produits ne disposent pas d'une interface utilisateur permettant aux clients de créer un lien avec leurs propres politiques et déclarations de protection des données.

17 Voir la section « Sécurité » pour plus d'informations.

18 Une fois un réseau ou système connecté à Internet, l'emplacement physique des données n'a que peu d'impact, voire aucun, sur les menaces de sécurité. Voir le livre blanc d'Amazon Web Services (AWS) « Data Residency AWS Policy Perspective » (en particulier les pages 2 et 3), qui donne des arguments convaincants contre la localisation des données.

19 À la date d'élaboration du présent document.

20 Voir les programmes de conformité d'AWS pour une liste complète des certifications et de la conformité légale.

21 Art. 28(2)-(4) du RGPD.

22 Art. 33 et 34 du RGPD.

23 Pour plus d'informations sur le rôle du sous-traitant, voir la section « Le rôle de votre organisation et de la nôtre vis-à-vis du RGPD ».

24 Voir la section « Démystifions le RGPD » pour plus d'informations sur les délais et le traitement des notifications de violation d'informations personnelles

25 Voir également la section « Contrats conclus avec des clients ».