(Traduction – Version septembre 2024)

Autorité belge de protection des données

Secrétariat Général

Les systèmes d'intelligence artificielle et le RGPD sous l'angle de la protection des données

Résumé

La présente brochure d'information décrit l'interaction complexe entre le Règlement général sur la protection des données (RGPD)[i] et le Règlement sur l'intelligence artificielle (IA)[ii] dans le contexte du développement des systèmes d'IA. Ce document souligne l'importance d'une mise en conformité des systèmes d'IA avec les principes de protection des données en vue de relever les défis uniques posés par les technologies d'IA.

Les points clés sont notamment les suivants :

- Alignement entre le RGPD et le règlement sur l'IA : la brochure souligne la complémentarité entre le RGPD et le règlement sur l'IA pour garantir un traitement de données à caractère personnel licite, loyal et transparent dans les systèmes d'IA.
- Définition d'un système d'IA : le présent document fournit une définition claire des systèmes d'IA ainsi que des exemples concrets afin de clarifier le concept.
- Principes de protection des données : la présente brochure approfondit les principes fondamentaux du RGPD tels que la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, l'exactitude, la limitation de la conservation et les droits des personnes concernées dans le contexte des systèmes d'IA.
- Responsabilité : l'importance de la responsabilité est mise en évidence, en exposant les exigences spécifiques du RGPD et du règlement sur l'IA.
- Sécurité : le présent document souligne la nécessité de mesures techniques et organisationnelles solides pour protéger les données à caractère personnel traitées par les systèmes d'IA.
- Contrôle humain : le rôle crucial d'un contrôle humain dans le développement et l'utilisation de systèmes d'IA est mis en avant, en particulier pour les systèmes d'IA à haut risque.

En donnant un aperçu du cadre juridique et en fournissant des conseils pratiques, la présente brochure d'information vise à permettre aux professionnels du droit, aux délégués à la protection des données et aux acteurs techniques, y compris les responsables du traitement et les sous-traitants, de comprendre et de respecter les exigences du RGPD et du règlement sur l'IA lors du développement et du déploiement de systèmes d'IA.

Objectif de la présente brochure d'information

Le Secrétariat Général de l'Autorité belge de protection des données surveille les développements sociétaux, économiques et technologiques ayant un impact sur la protection des données à caractère personnel[iii].

Ces dernières années, les technologies d'IA ont connu une croissance exponentielle, révolutionnant plusieurs industries et impactant de façon significative la manière dont les données sont collectées, traitées et utilisées. Toutefois, ce développement rapide a engendré des défis complexes en matière de confidentialité des données, de transparence et de responsabilité (« accountability »).

Dans ce contexte, le Secrétariat Général de l'Autorité belge de protection des données publie la présente brochure d'information afin de donner un aperçu de la protection des données ainsi que du développement et du déploiement de systèmes d'IA.

Comprendre et respecter les principes et les dispositions du RGPD est crucial pour garantir un fonctionnement éthique, responsable et conforme aux normes juridiques des systèmes d'IA. La présente brochure d'information vise à expliquer les exigences du RGPD spécifiquement applicables aux systèmes d'IA en proposant des informations utiles et les plus claires possibles aux acteurs impliqués dans le développement, le déploiement et la réglementation (interne) de technologies d'IA.

En plus du RGPD, l'Artificial Intelligence Act (règlement sur l'IA), qui est entré en vigueur le 1er août 2024, aura également un impact significatif sur la réglementation du développement et de l'utilisation de systèmes d'IA. La présente brochure d'information abordera également les exigences du règlement sur l'IA.

Public cible de la présente brochure d'information

La présente brochure d'information s'adresse à un public diversifié, incluant les professionnels du droit, les délégués à la protection des données (Data Protection Officers ou DPO) ainsi que les personnes ayant une formation technique, telles que les analystes fonctionnels, les architectes et les développeurs. Elle cible également les responsables du traitement et les sous-traitants impliqués dans le développement et le déploiement de systèmes d'IA. Vu le croisement de considérations juridiques et techniques inhérent à l'application du RGPD aux systèmes d'IA, la présente brochure d'information vise à combler le fossé entre les exigences légales et la mise en œuvre technique.

Les professionnels du droit et les DPO jouent un rôle crucial dans la garantie d'une conformité organisationnelle avec les obligations du RGPD, en particulier celles qui concernent les systèmes d'IA qui traitent des données à caractère personnel. En donnant un aperçu des exigences du RGPD spécifiques à l'IA, la présente brochure d'information procure aux professionnels du droit et aux DPO des connaissances utiles pour se repérer dans les complexités des activités de traitement de données en lien avec l'IA, évaluer les risques et mettre en œuvre des mesures appropriées.

En même temps, les personnes ayant une formation technique telles que les analystes fonctionnels, les architectes et les développeurs font partie intégrante de la conception, du développement et du déploiement de systèmes d'IA. Reconnaissant leur rôle central, la présente brochure d'information vise à clarifier les exigences du RGPD d'une manière accessible aux acteurs techniques. Le texte comprend des exemples concrets, tirés de la vie réelle, afin d'illustrer comment les principes du RGPD se traduisent en considérations pratiques pendant le cycle de vie des projets d'IA. En fournissant des informations utiles, la présente brochure d'information permet aux professionnels techniques de concevoir des systèmes d'IA conformes aux obligations du RGPD, d'intégrer les principes de protection des données dès la conception et d'atténuer les risques juridiques et éthiques potentiels.

Qu'est-ce qu'un système d'IA ?

Les termes "système d'IA" recouvrent un large éventail d'interprétations.

La présente brochure d'information n'approfondira pas les subtilités et les nuances qui distinguent ces différentes définitions.
Elle commencera plutôt par examiner la définition d'un système d'IA, telle que reprise dans le règlement sur l'IA[iv]:

Aux fins du présent règlement, on entend par :
(1) "système d'IA", un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels;

Autrement dit :
Un système d'IA est un système informatique spécifiquement conçu pour analyser des données, identifier des modèles et utiliser cette connaissance pour générer des décisions ou des prédictions informées.
Dans certains cas, les systèmes d'IA peuvent apprendre à partir des données et s'adapter au fil du temps. Cette capacité d'apprentissage leur permet d'améliorer leurs performances, d'identifier des modèles complexes dans différents ensembles de données et de générer des décisions plus précises ou plus nuancées.

Exemples de systèmes d'IA dans la vie quotidienne :

Filtres anti-spam dans les e-mails : les filtres anti-spam analysent les e-mails entrants et identifient les modèles qui distinguent les spams des e-mails légitimes. Au fil du temps, le marquage d'e-mails par les utilisateurs en tant que spam ou non spam permet au système d'IA d'apprendre et d'améliorer la précision de son filtrage. Il s'agit d'un exemple d'un système d'IA qui rencontre les critères d'un système d'IA :

- système automatisé : il s'agit d'un programme informatique ;
- qui analyse des données : il analyse le contenu des e-mails ;
- qui identifie des modèles : il identifie dans les e-mails des modèles qui suggèrent des spams ;

- qui génère des décisions : il décide de catégoriser un e-mail en tant que spam ou non.

Systèmes de recommandations dans les services de streaming : les services de streaming de films utilisent des systèmes d'IA pour générer des recommandations pour les utilisateurs. Ces systèmes analysent les habitudes passées de visionnage d'un utilisateur ainsi que les habitudes d'utilisateurs similaires pour recommander du contenu susceptible de les intéresser. Cela constitue un autre exemple de système d'IA :

- système automatisé : il s'agit d'un programme informatique ;
- qui analyse des données : il analyse l'historique de visionnage/d'écoute d'un utilisateur ;
- qui identifie des modèles : il identifie des modèles dans les préférences de l'utilisateur et celles d'utilisateurs similaires ;
- qui génère des recommandations : il recommande du contenu basé sur les modèles identifiés.

Assistants virtuels : les assistants virtuels répondent à des commandes vocales et exécutent des tâches telles que régler une alarme, diffuser de la musique ou contrôler des appareils domestiques intelligents. Ces systèmes utilisent la reconnaissance vocale et le traitement automatique des langues pour comprendre les requêtes des utilisateurs et y répondre. Il s'agit à nouveau d'un exemple de système d'IA :

- système automatisé : il s'agit d'un programme informatique ;
- qui analyse des données : il analyse les commandes vocales de l'utilisateur ;
- qui identifie des modèles : il identifie des modèles dans le discours pour comprendre les requêtes de l'utilisateur ;
- il génère des décisions : il décide comment répondre aux commandes en se basant sur sa compréhension ;
- il peut faire preuve de capacité d'adaptation : certains assistants virtuels peuvent apprendre les préférences de l'utilisateur et adapter leurs réponses au fil du temps.

Analyse d'imagerie médicale par l'IA : de nombreux hôpitaux et prestataires de soins de santé utilisent des systèmes d'IA pour aider les médecins à analyser des images médicales, telles que des radiographies, des scanners et des IRM. Ces systèmes sont entraînés sur de vastes ensembles de données d'images médicales, ce qui leur permet d'identifier des modèles et d'éventuelles anomalies.

- système automatisé : il s'agit d'un programme informatique ;
- qui analyse des données : il analyse les images médicales numériques ;

- qui identifie des modèles : il identifie des modèles dans les images pouvant indiquer la présence d'une maladie ou d'une anomalie ;
- il soutient la prise de décision : ce système met en évidence les zones potentiellement préoccupantes de l'image, ce qui peut aider les médecins à poser des diagnostics plus éclairés.

Exigences du RGPD et du règlement sur l'IA

Traitement licite, loyal et transparent

Le RGPD exige licéité, loyauté et transparence.

Licéité du traitement en vertu du RGPD : le RGPD définit six bases juridiques pour le traitement de données à caractère personnel (consentement, contrat, obligation légale, intérêt vital, mission d'intérêt public et intérêt légitime). Ces mêmes bases juridiques demeurent applicables aux systèmes d'IA qui traitent des données à caractère personnel en vertu du règlement sur l'IA.

Systèmes d'IA interdits : le règlement sur l'IA introduit d'autres interdictions allant au-delà du RGPD pour certains systèmes d'IA à haut risque. Tandis que le RGPD se concentre sur la protection des données à caractère personnel par le biais de différents principes, le règlement sur l'IA interdit directement des types spécifiques d'applications d'IA à haut risque. En voici quelques exemples :

- Systèmes de notation sociale : ces systèmes attribuent une note à des personnes, basée sur différents facteurs, menant potentiellement à la discrimination et à la limitation des opportunités.
- Systèmes d'IA pour la reconnaissance faciale en temps réel dans des lieux publics (avec des exceptions limitées) : ces systèmes suscitent des préoccupations au niveau du respect de la vie privée, de la liberté de mouvement et des abus potentiels en matière de surveillance de masse.

Loyauté :

- Bien que le règlement sur l'IA ne comprenne pas de section intitulée "loyauté", il s'appuie sur le principe de loyauté du traitement du RGPD (l'article 5.1.a), car le règlement sur l'IA se concentre sur l'atténuation des biais et de la discrimination dans le développement, le déploiement et l'utilisation de systèmes d'IA.

Transparence:

- Le règlement sur l'IA exige un niveau de base de transparence pour tous les systèmes d'IA. Cela signifie que les utilisateurs devraient être informés du fait qu'ils interagissent avec un système d'IA. Par exemple, un agent conversationnel ou chatbot pourrait entamer une interaction avec un message tel que "Bonjour, je suis Nelson, un **chatbot**. Comment puis-je vous aider aujourd'hui ?"
- Pour les systèmes d'IA à haut risque, le règlement sur l'IA exige un niveau de transparence plus élevé. Cela inclut la communication d'informations claires et

accessibles sur la manière dont les données sont utilisées dans ces systèmes, en particulier en ce qui concerne le processus décisionnel. Les utilisateurs devraient comprendre les facteurs qui influencent les décisions basées sur l'IA et la manière dont de potentiels biais sont atténués.

Limitation des finalités et minimisation des données

Le RGPD exige la limitation des finalités (art. 5.1.b) et la minimisation des données (art. 5.1.c). Cela signifie que les données à caractère personnel doivent être collectées pour des finalités déterminées et légitimes, et limitées à ce qui est nécessaire pour atteindre ces finalités. Ces principes garantissent que les systèmes d'IA n'utilisent pas de données pour des finalités autres que celles pour lesquelles ils ont été conçus ou qu'ils ne collectent pas de données excessives.
Le règlement sur l'IA renforce le principe de limitation des finalités - issu du RGPD - pour les systèmes d'IA à haut risque en mettant l'accent sur la nécessité d'une finalité bien définie et documentée.

Exemple : Un système d'IA d'approbation de prêt d'une institution financière utilise, outre les données d'identification standards et les informations du bureau de crédit, également des données de géolocalisation (par ex. les lieux visités précédemment) et des données de médias sociaux (par ex. les profils d'amis et les intérêts) d'une personne concernée. Cette collecte étendue de données, incluant des données de géolocalisation et des données de médias sociaux, soulève des préoccupations quand à la conformité du système avec le règlement sur l'IA.

Exactitude et actualité des données

Le RGPD exige que les données à caractère personnel soient exactes et, si nécessaire, tenues à jour (art. 5.1.d). Les organisations doivent prendre des mesures raisonnables pour le garantir. Le règlement sur l'IA s'appuie sur ce principe en exigeant que les systèmes d'IA à haut risque utilisent des données de haute qualité et objectives pour éviter tout résultat discriminatoire.

Exemple : une institution financière développe un système d'IA pour automatiser les approbations de prêts. Le système analyse différents points de données concernant les demandeurs de prêt, notamment les antécédents de crédit, les revenus et les données démographiques (code postal). Cependant, les données d'entraînement du système d'IA reflètent à leur insu des biais historiques : les données proviennent d'une période où les

prêts étaient plus facilement octroyés dans les quartiers plus aisés (avec un revenu moyen plus élevé). Le système d'IA perpétue ces biais car les demandeurs de prêt issus de quartiers à faibles revenus peuvent se voir systématiquement refuser des prêts, même s'ils remplissent les conditions financières. Cela aboutit à un résultat discriminatoire et peut soulever de sérieuses préoccupations quant à la conformité du système avec le règlement sur l'IA.

Limitation de la durée de conservation

Le RGPD exige que les données à caractère personnel ne soient pas conservées plus longtemps que le temps nécessaire à l'accomplissement des finalités pour lesquelles elles ont été collectées (art. 5.1.e). Le règlement sur l'IA n'introduit pas explicitement d'autre exigence ou d'exigence supplémentaire concernant la limitation de la conservation pour les systèmes d'IA à haut risque.

Prise de décision automatisée

Le RGPD et le règlement sur l'IA abordent tous deux l'importance de l'intervention humaine dans les processus de prise de décision automatisée impactant des personnes. Cependant, ils diffèrent par leur approche :

- Le RGPD accorde aux personnes le droit de ne pas faire l'objet d'une décision uniquement fondée sur un traitement automatisé produisant des décisions juridiques les concernant (art. 22). Cela implique que les personnes concernées ont le droit de demander le réexamen d'une décision automatisée par un décideur humain. Il s'agit d'un droit individuel de contester les décisions perçues comme injustes ou inexactes.
- Le règlement sur l'IA renforce l'accent mis sur l'implication humaine en exigeant un contrôle humain significatif tout au long du développement, du déploiement et de l'utilisation de systèmes d'IA à haut risque. Il s'agit d'une mesure de gouvernance visant à garantir un développement et une utilisation responsables de l'IA. En vertu du règlement sur l'IA, le contrôle humain englobe un ensemble d'activités plus large que le simple réexamen de décisions individuelles. Il inclut, par exemple, le réexamen des données d'entraînement et des algorithmes des systèmes d'IA pour y déceler d'éventuels biais, la surveillance des performances du système et l'intervention dans les processus décisionnels cruciaux.

En substance, le RGPD permet aux personnes de s'opposer à des décisions uniquement automatisées, tandis que le règlement sur l'IA exige un contrôle humain proactif des systèmes d'IA à haut risque afin de se prémunir contre des biais potentiels et d'assurer un développement et une utilisation responsables de ces systèmes.

Exemple : une agence gouvernementale utilise un système d'IA pour évaluer l'éligibilité à des prestations sociales en fonction des revenus, de la situation professionnelle et de la situation familiale.
En vertu du RGPD, les personnes ont le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé pour déterminer leur éligibilité à des prestations sociales (art. 22). Cela signifie qu'elles peuvent demander un réexamen d'une décision automatisée par un décideur humain.
En vertu du règlement sur l'IA, ce système d'IA est classifié en tant que système à haut risque (car il a un impact significatif sur les moyens de subsistance des personnes). L'agence gouvernementale doit donc mettre en place un contrôle humain tout au long du développement, du déploiement et de l'utilisation du système d'IA.

Sécurité du traitement

Le RGPD et le règlement sur l'IA soulignent tous deux l'importance de sécuriser les données à caractère personnel tout au long de leur traitement. Toutefois, les systèmes d'IA présentent des risques spécifiques qui nécessitent des mesures de sécurité supplémentaires allant au-delà des pratiques traditionnelles de protection des données.

Le RGPD impose aux organisations de mettre en oeuvre des mesures techniques et organisationnelles (MTO) appropriées au risque associé à leurs activités de traitement de données. Cela implique d'évaluer les risques afin d'identifier les menaces et les vulnérabilités potentielles. Les MTO choisies devraient atténuer ces risques et garantir un niveau de sécurité de base pour les données à caractère personnel.

Le règlement sur l'IA s'appuie sur cette base en imposant des mesures de sécurité solides pour les systèmes d'IA à haut risque. En effet, les systèmes d'IA présentent des risques spécifiques qui vont au-delà du traitement traditionnel de données, comme par exemple :

- biais potentiels dans les données d'entraînement : des données d'entraînement biaisées peuvent donner lieu à des décisions biaisées par le système d'IA, impactant injustement les personnes ;

- manipulation par des personnes non autorisées : par exemple, un hacker pourrait manipuler les données d'entraînement du système d'IA afin d'influencer ses décisions de manière préjudiciable. Imaginez qu'un système entraîné pour approuver des demandes de prêt soit dupé pour être amené à rejeter des candidats qualifiés sur la base de facteurs non pertinents.

Pour faire face à ces risques particuliers, le règlement sur l'IA met l'accent sur des mesures proactives telles que :

- l'identification et la planification des problèmes potentiels : ceci implique de réfléchir à ce qui pourrait mal se passer avec le système d'IA et à la probabilité que cela se produise (évaluation des risques). Il s'agit d'une pratique essentielle en vertu tant du RGPD que du règlement sur l'IA.
- surveillance et tests continus : ceci implique d'évaluer régulièrement les performances du système d'IA en fonction de plusieurs aspects, notamment :
    - les failles de sécurité : identification des vulnérabilités dans le code ou la conception du système qui pourraient être exploitées par des 'agresseurs'.
    - biais : vérification des biais potentiels dans les données d'entraînement du système ou dans les processus décisionnels.
- contrôle humain : le règlement sur l'IA souligne l'importance d'un contrôle humain significatif tout au long du développement, du déploiement et de l'utilisation de systèmes d'IA à haut risque. Cela permet de s'assurer que des humains sont impliqués dans les décisions cruciales et qu'ils comprennent les vulnérabilités du système. Le contrôle humain prévu par le règlement sur l'IA va au-delà des seuls processus de sécurité et englobe divers aspects, tels que :
    - le réexamen des données d'entraînement et des algorithmes afin de détecter d'éventuels biais ;
    - le contrôle des performances du système en termes d'équité, d'exactitude et de conséquences involontaires potentielles ;
    - l'intervention dans les processus décisionnels cruciaux, en particulier lorsqu'ils peuvent avoir un impact significatif sur les personnes.

Exemple : Système de diagnostic du cancer du poumon basé sur l'IA.

Un système d'IA utilisé par un hôpital pour diagnostiquer le cancer du poumon est un exemple de système d'IA à haut risque en raison de plusieurs facteurs :

- données hautement sensibles : il traite des données à caractère personnel hautement sensibles, dont des informations sur la santé des patients (poumons) et des diagnostics (catégorie particulière de données en vertu de l'article 9 du RGPD) ;

- impact d'une fuite de données : une fuite de données pourrait exposer des informations cruciales sur la santé des patients, pouvant mener à des violations de la vie privée et à une atteinte à la réputation de l'hôpital ;
- décisions qui changent la vie : le résultat du système impacte directement la vie des patients. Un diagnostic basé sur des données inexactes ou compromises peut avoir de graves conséquences pour leur santé et leur bien-être.

Le RGPD et le règlement sur l'IA soulignent tous deux l'importance de mesures de sécurité pour les activités de traitement de données, en particulier celles impliquant des données sensibles :

- Le RGPD établit une base pour la sécurité des données : il exige des organisations qu'elles mettent en œuvre les mesures techniques et organisationnelles (MTO) appropriées afin de protéger les données à caractère personnel sur la base d'une évaluation des risques. Pour les données relatives à la santé, ces mesures seraient particulièrement strictes en raison de leur caractère sensible. Les exemples en vertu du RGPD pourraient être les suivants :
  - le chiffrement des données : le chiffrement des données des patients, au repos et en transit, garantit leur confidentialité même en cas de fuite de données ;
  - contrôles des accès : la mise en oeuvre de contrôles des accès stricts limite les personnes autorisées à accéder aux données des patients et à les modifier ;
  - test de pénétration : la réalisation régulière de tests de pénétration permet d'identifier et de traiter les vulnérabilités du dispositif de sécurité du système ;
  - la journalisation et l'audit : le maintien d'une journalisation détaillée de l'activité du système permet de surveiller et d'enquêter sur tout comportement suspect.
- Le règlement sur l'IA s'appuie sur cette base pour les systèmes d'IA à haut risque : reconnaissant les risques spécifiques de l'IA, le règlement sur l'IA impose des mesures de sécurité solides. Il peut s'agir de mesures supplémentaires adaptées aux vulnérabilités spécifiques du système d'IA, telles que la validation des données et l'assurance de leur qualité : le règlement sur l'IA souligne l'importance de garantir la qualité et l'intégrité des données utilisées pour entraîner et faire fonctionner le système d'IA. Cela pourrait impliquer des techniques en lien avec :
  - la provenance des données : suivre l'origine des données afin d'identifier les sources potentielles de biais ou de manipulation dans les données d'entraînement, telles qu'un étiquetage incorrect des rayons X ;

- la détection d'anomalies : identifier et signaler les schémas inhabituels dans les données d'entraînement qui pourraient indiquer une manipulation malveillante, comme un afflux soudain de radiographies présentant des caractéristiques irréalistes ;
- le contrôle humain des points de données à haut risque : faire contrôler les radiographies cruciales par des professionnels de la santé avant qu'elles ne soient utilisées pour entraîner le système d'IA, en particulier celles qui présentent des caractéristiques inhabituelles ou qui pourraient avoir un impact significatif sur les résultats du patient.

La mise en œuvre de ces mesures de sécurité permet à l'hôpital d'atténuer les risques associés au système de diagnostic du cancer du poumon basé sur l'IA et de garantir la vie privée des patients, la sécurité des données et, en fin de compte, d'assurer les meilleurs résultats possibles pour les patients.

Droits de la personne concernée

Le RGPD octroie aux personnes physiques des droits de la personne concernée qui leur permettent de contrôler leurs données à caractère personnel et la manière dont elles sont utilisées. Ces droits incluent l'accès (voir quelles données sont traitées, art. 15), la rectification (corriger les données inexactes et compléter des données, art. 16), l'effacement (demander l'effacement de données, art. 17), la limitation du traitement (limiter la manière dont les données sont utilisées, art. 18) et la portabilité des données (transmettre des données à un autre service, art. 20).
Afin d'exercer concrètement ces droits, les personnes physiques ont besoin de comprendre de quelle manière leurs données sont utilisées. Le règlement sur l'IA renforce cet aspect en soulignant l'importance d'explications claires sur la manière dont les données sont utilisées dans les systèmes d'IA. Grâce à cette transparence, les personnes peuvent prendre des décisions éclairées concernant leurs données et exercer leurs droits plus efficacement.

Exemple : un système d'IA utilisé pour déterminer des primes d'assurance automobile octroie une prime relativement élevée à un client particulier (personne concernée). Le règlement sur l'IA accorde à ce client le droit de recevoir une explication claire sur la manière dont la prime est calculée. Par exemple, l'assureur (responsable du traitement) pourrait expliquer que différents points de données ont été utilisés, tels que le kilométrage annuel du client, ses antécédents d'accidents et si le véhicule est utilisé à des fins

professionnelles. Ces informations permettent à leur tour au client d'exercer ses droits de personne concernée en vertu du RGPD, tels que le droit de rectification (corriger des données à caractère personnel inexactes ou compléter des données à caractère personnel).

Responsabilité

Le RGPD impose (que les organisations démontrent) la responsabilité du traitement de données à caractère personnel au travers de plusieurs mesures telles que :

- la transparence du traitement : les personnes doivent comprendre comment leurs données sont collectées, utilisées, conservées et partagées (par ex. par le biais d'une politique de protection de la vie privée claire et concise, grâce au droit d'accès de la personne concernée, ...) Cette transparence leur permet de voir si leurs données sont traitées de manière licite et loyale ;
- Politiques et procédures pour le traitement de données à caractère personnel : des politiques documentées garantissent des pratiques de traitement de données cohérentes dans toute l'organisation ;
- Base juridique documentée pour le traitement : pour chaque activité de traitement de données, les organisations ont besoin de preuves documentées de la justification légale (consentement, contrat, intérêt légitime, etc.) ;
- La tenue de différents registres (tels que le registre des activités de traitement, des demandes des personnes concernées, des fuites de données) est requise : conserver des registres exacts témoigne d'un engagement des organisations à rendre des comptes et leur permet également de prouver leur conformité lors d'audits ou d'enquêtes ;
- Mesures de sécurité : mettre en œuvre et appliquer correctement des mesures techniques et organisationnelles appropriées (MTO) pour protéger les données à caractère personnel est essentiel pour démontrer la responsabilité ;
- Dans certains cas, une analyse d'impact relative à la protection des données (AIPD) est requise : elle est obligatoire lors du traitement de données à haut risque ou du déploiement de nouvelles technologies ;
- Un délégué à la protection des données (DPO) est requis dans certains cas : par ex. les organisations gouvernementales, quelles que soient leurs activités principales, sont tenues d'avoir un DPO.

Bien que le règlement sur l'IA ne comprenne pas de section consacrée à la preuve de la responsabilité, il s'appuie sur les principes du RGPD. Le règlement sur l'AI exige que les organisations mettent en œuvre :

- une approche de la gestion des risques en deux étapes pour les systèmes d'IA. Il y a tout d'abord un premier processus de classification qui catégorise le risque que l'IA représente pour les personnes (allant de minimal à élevé).
  Pour les systèmes présentant un risque élevé, une évaluation du risque plus approfondie est requise. Celle-ci analyse les risques spécifiques plus en profondeur et identifie les dommages potentiels associés au système d'IA, et est également appelée analyse d'impact sur les droits fondamentaux (ou FRIA (Fundamental Rights Impact Assessment)) ;
- une documentation claire de la conception et du déploiement des systèmes d'IA ;
- des processus soumis à un contrôle humain dans les systèmes d'IA à haut risque. Cela pourrait impliquer une intervention ou une approbation humaines des décisions cruciales prises par le système d'IA ;
- une procédure formelle de signalement des incidents liés à des dysfonctionnements du système d'IA ou à des conséquences involontaires.

Simplifier la conformité : des récits utilisateurs ou *user stories* pour les systèmes d'IA à la lumière du RGPD et des exigences du règlement sur l'IA

Traduire les exigences réglementaires en spécifications techniques pour les systèmes d'IA présente des défis importants. La présente brochure se concentre sur l'utilisation de *user stories* pour combler le fossé entre les obligations légales et le développement du système.

Les *user stories* offrent une approche pratique pour comprendre et aborder les exigences réglementaires dans le contexte de la conception d'un système d'IA. En adoptant une perspective centrée sur l'utilisateur, les organisations peuvent traduire efficacement les obligations légales en mesures concrètes.

La présente brochure utilise un système de calcul des primes d'assurance automobile comme exemple pour illustrer l'application des *user stories* dans le domaine de l'IA.

Exigences d'un traitement licite, loyal et transparent

User story : garantir la licéité - base légale correcte

En tant que compagnie d'assurance ayant recours à un système d'IA pour le calcul des primes automobiles, nous devons procéder à une analyse approfondie de la base légale afin de déterminer la justification légale la plus appropriée pour collecter et utiliser des données clients dans notre système d'IA. C'est important pour agir conformément au principe de licéité du RGPD.

User story : garantir la licéité - données interdites

En tant que compagnie d'assurance ayant recours à un système d'IA pour le calcul des primes automobiles, nous devons nous assurer que notre système respecte les interdictions du RGPD et du règlement sur l'IA de traiter certains types de données à caractère personnel. Ces interdictions incluent des catégories particulières de données à caractère personnel telles que l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses, etc. C'est important pour se conformer à la protection des données à caractère personnel sensibles prévue par le RGPD et à la prévention des résultats discriminatoires mise en avant par le règlement sur l'IA.

User story : garantir la loyauté

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes automobiles, nous devons garantir un traitement loyal et non discriminatoire des données clients. C'est important pour se conformer au principe de loyauté du RGPD et à l'accent spécifique que le règlement sur l'IA met sur la prévention de résultats biaisés qui pourraient désavantager certains groupes.

La compagnie d'assurance automobile peut garantir la loyauté par les moyens suivants :

- examiner les sources de données : analyser les sources de données utilisées pour entraîner le système d'IA afin d'identifier et d'atténuer les biais potentiels basés sur des facteurs tels que le code postal, le sexe, l'âge, … . Veiller à ce que ces facteurs soient utilisés de manière pertinente et nécessaire pour le calcul des primes, en évitant tout résultat discriminatoire ;
- tester la loyauté : tester régulièrement le système d'IA sur la présence de biais potentiels dans ses résultats. Ceci peut impliquer de comparer des calculs de prime automobile pour des profils clients similaires afin d'identifier des différences inexplicables ;

- un contrôle humain : mettre en œuvre un processus de contrôle humain pour des décisions ayant un impact élevé qui ont été prises par le système d'IA, telles que des augmentations sensibles de primes automobiles ou même des refus de police.

User story : garantir la transparence

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes automobiles, nous devons être transparents quant à la manière dont les données de nos clients sont utilisées. C'est important pour se conformer au principe de transparence du RGPD et à l'accent spécifique que le règlement sur l'IA met sur la transparence pour les systèmes d'IA à haut risque.

La compagnie d'assurance automobile peut garantir la transparence par les moyens suivants :

- une déclaration de protection des données : expliquer clairement dans la déclaration de protection des données de l'entreprise comment les données clients sont collectées, utilisées et conservées dans le système d'IA pour le calcul des primes ;
- des explications faciles à comprendre : fournir des explications claires pour le client sur le processus de calcul des primes basé sur l'IA. Cela peut impliquer d'utiliser un langage simple, des images ou des FAQ pour démystifier le rôle de l'IA dans la détermination des primes d'assurance automobile ;
- le droit d'accès à l'information : mettre en place des mécanismes permettant aux clients d'accéder facilement aux informations sur les points de données utilisés dans le calcul spécifique de leur prime.

Exigences d'une limitation des finalités et d'une minimisation des données

User story : garantir la limitation des finalités

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons veiller à ce que les données que nous collectons auprès de nos clients se limitent au strict nécessaire pour le calcul précis des primes. C'est important pour agir conformément au principe de licéité du RGPD.

User story : garantir la minimisation des données

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons appliquer une stratégie de minimisation des données afin de veiller à ne collecter et à n'utiliser que le nombre minimum de données clients

nécessaires pour le calcul précis des primes. C'est important pour agir conformément au principe de minimisation du RGPD.

Exigences d'exactitude et d'actualité des données

User story : garantir l'exactitude et l'actualité des données

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons mettre en place des processus pour garantir l'exactitude et l'actualisation des données clients utilisées dans le système. C'est important pour agir conformément au principe d'exactitude du RGPD.

La compagnie d'assurance automobile peut assurer l'exactitude et l'actualité des données clients via :

- des mécanismes de vérification des données : proposer aux clients des mécanismes faciles à utiliser pour vérifier et mettre à jour leurs données à caractère personnel dans le système d'assurance automobile. Il peut s'agir d'un portail en ligne, d'une application mobile ou d'une ligne téléphonique spécifique ;
- une actualisation régulière des données : établir des procédures pour actualiser régulièrement les données clients utilisées dans le système d'IA. Il peut s'agir de demander aux clients d'actualiser périodiquement leurs informations ou d'une intégration à des sources de données externes (par exemple, des bases de données de dossiers de conduite) pour mettre à jour automatiquement les points de données pertinents ;
- des alertes qualité quotidiennes : mettre en place des alertes pour les points de données manquants ou potentiellement inexacts dans les profils des clients. Cela permet à l'entreprise de contacter les clients de manière proactive et de leur demander des mises à jour ;
- une communication claire aux clients sur leur droit de rectification en vertu du RGPD. Ce droit leur permet de demander la rectification de toute donnée à caractère personnel inexacte ou de compléter les données manquantes utilisées dans le système de calcul des primes.

User story : garantir l'utilisation de données non biaisées

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons nous assurer que les données utilisées pour entraîner et faire fonctionner le système sont exemptes de biais. C'est important pour se conformer à l'accent spécifique que le règlement sur l'IA met sur la prévention de résultats biaisés qui pourraient désavantager certains groupes.

La compagnie d'assurance automobile peut obtenir des données non biaisées pour un calcul équitable de la prime d'assurance automobile basé sur l'IA via :

- une évaluation de la source des données : analyser la source des données utilisées pour entraîner le système d'IA. Identifier les biais potentiels basés sur des facteurs tels que l'origine socio-économique dans le processus de collecte des données ;
- une surveillance régulière et un test des biais : surveiller en permanence les performances du système d'IA afin de déceler d'éventuels biais dans ses résultats. Tester régulièrement la présence de biais afin d'identifier et de traiter tout résultat discriminatoire dans le calcul des primes ;
- un contrôle humain : mettre en œuvre un processus de contrôle humain pour des décisions ayant un impact élevé qui ont été prises par le système d'IA, telles que des augmentations sensibles de primes automobiles ou même des refus de police. Cela permet une intervention humaine pour éviter les résultats biaisés ;
- de la transparence vis-à-vis des clients : informer les clients, dans la déclaration de protection des données, de l'engagement de l'entreprise à utiliser des données de haute qualité et non biaisées dans le système d'IA.

Exigence de sécurité du traitement

User story : mettre en place des mesures de sécurité appropriées pour l'assurance automobile basée sur l'IA

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons procéder à une évaluation approfondie des risques afin d'identifier les menaces et les vulnérabilités potentielles qui pourraient avoir un impact sur les données de nos clients. Cette évaluation prendra en compte différents facteurs, notamment le type de données (données financières ou informations de base sur les clients), les activités de traitement et l'impact potentiel d'une faille de sécurité. Sur la base de cette évaluation, nous mettrons en œuvre des mesures techniques et organisationnelles (MTO) appropriées pour atténuer ces risques et garantir la sécurité des données de nos clients. C'est important pour se conformer aux exigences de sécurité du traitement en vertu du RGPD.

Parmi les exemples de MTO, nous pouvons citer :

- le chiffrement des données : chiffrer les données des clients, au repos et en transit, pour en garantir la confidentialité ;
- le contrôles des accès : mettre en place des contrôles des accès stricts pour limiter les personnes autorisées à accéder aux données clients et à les modifier ;
- les tests de pénétration réguliers : réaliser des tests de pénétration afin d'identifier et de traiter les vulnérabilités du dispositif de sécurité du système ;
- la journalisation et l'audit : maintenir une journalisation détaillée de l'activité du système afin de surveiller et d'enquêter sur tout comportement suspect.

User story : gérer les risques spécifiques dans le système d'assurance automobile basé sur l'IA

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes automobiles, nous reconnaissons que les systèmes d'IA présentent des risques spécifiques au-delà du traitement traditionnel des données. Ces risques peuvent inclure des biais potentiels dans les données d'entraînement ou des manipulations par des acteurs non autorisés. Pour faire face à ces risques spécifiques, nous mettrons en œuvre des mesures supplémentaires conjointement avec les MTO de base conformes au RGPD. C'est important pour se conformer aux exigences de sécurité du traitement en vertu du RGPD.

Parmi les exemples de mesures supplémentaires on peut citer :

- la validation des données et l'assurance de leur qualité : mettre en œuvre des procédures pour garantir la qualité et l'intégrité des données utilisées pour entraîner et faire fonctionner le système d'IA. Il peut s'agir de suivre la provenance des données et de détecter les anomalies afin d'identifier des biais potentiels ou des tentatives de manipulation ;
- le contrôle humain : mettre en place un cadre pour le contrôle humain tout au long du cycle de vie du système d'IA. Il peut s'agir d'un contrôle humain des points de données à haut risque, d'une surveillance de l'équité et de l'exactitude des performances du système et d'une intervention dans les processus décisionnels cruciaux.

Exigence de (capacité à démontrer sa) responsabilité

User story : documenter la base juridique

En tant que compagnie d'assurance ayant recours à un système d'IA pour le calcul des primes automobiles, nous devons disposer d'un rapport clair et concis de la base légale pour la collecte et l'utilisation des données clients dans notre système d'IA. C'est important pour se conformer au principe de (capacité à démontrer sa) responsabilité du RGPD (également dans le contexte d'audits ou d'enquêtes).

User story : réaliser une analyse d'impact sur les droits fondamentaux (ou Fundamental Rights Impact Assessment (FRIA))

En tant que compagnie d'assurance automobile ayant recours à un système d'IA pour le calcul des primes, nous devons élaborer et maintenir une analyse d'impact détaillée sur les droits fondamentaux (Fundamental Rights Impact Assessment (FRIA)) afin d'identifier et d'atténuer de manière proactive les risques potentiels associés à ce système d'IA. C'est important pour se conformer aux exigences du règlement sur l'IA pour les systèmes d'IA à haut risque et promouvoir des calculs de primes équitables et non discriminatoires pour nos clients.

Bibliographie

[0] La version originale en anglais du présent document a fait l'objet d'une vérification orthographique et grammaticale et a utilisé un Large Language Model ou grand modèle de langage, comme outil pour affiner et corriger les sections de texte initiales.
[i] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données),Journal officiel de l'Union européenne L 119/1, 4.5.2016, p. 1–88.
[ii] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 *établissant des règles harmonisées concernant l'intelligence artificielle* (règlement sur l'intelligence artificielle), Journal officiel de l'Union européenne L 199/1, 12.7.2024, p. 1–120.
[iii] Art. 20, § 1er, 1° de la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, modifiée par la loi du 25 décembre 2023.
[iv] Règlement sur l'intelligence artificielle, article 3 (1).