Directive RGPD
Déclaration de politique générale

Contexte

Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données (RGPD), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

En Belgique, il est complété par la loi-cadre du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel qui a abrogé l'ancienne loi du 8 décembre 1992 et ses arrêtés royaux d'exécution.

Le RGPD est applicable pour toutes les personnes et toutes les ressources impliquées dans l'ensemble des activités et métiers d'ORES.

Conformément au principe de RESPONSABILITE (accountability), ORES doit pouvoir garantir et prouver sa conformité en matière de protection des données à caractère personnel à tout moment.

Le Comité de direction d'ORES a opté pour une approche pragmatique de la conformité au RGPD fondée sur un équilibre des risques où il est tenu compte des particularités liées à la mission de service public d'ORES et aux obligations légales de maitrise des coûts.

Objet

Pour l'exercice de sa mission de service public, de ses obligations légales et de ses missions annexes, ORES collecte, détient et manipule une gigantesque quantité de données à caractère personnel relative à ses clients, employés et partenaires divers.

En tant que responsable de traitement des données et en tant que sous-traitant de données, ORES a entamé dès 2017 un important processus de mise en conformité aux obligations du RGPD. Il s'agit d'un processus constant d'amélioration en fonction des prises de position et recommandations de l'Autorité de Protection des Données ou des instances européennes, ainsi que de la jurisprudence.

L'évolution des technologies, les nouveaux enjeux du secteur et l'adaptation constante des environnements de travail font apparaitre de nouveaux risques et défis qui ne doivent pas remettre en cause la volonté d'ORES d'innover dans le respect des droits de chacun.

Notes de version et diffusion

VERSION : N° 4 du 2/04/2024

NOTES DE MISE À JOUR : CETTE POLITIQUE DOIT ÊTRE REMISE ANNUELLEMENT À JOUR PAR LE DPO, LES MODIFICATIONS SERONT SOUMISES AU CD.

DATE DE PREMIÈRE MISE EN APPLICATION : 1/03/2019

POUR MISE EN APPLICATION : TOUT ORES

POUR INFORMATION : **TOUT ORES**

	NOMS	DATE – SIGNATURE
RÉDACTEUR	Vinciane Royez	
RESPONSABLE DU PROCESSUS	Vinciane Royez	
DIRECTION	Fernand Grifnée	
	Nicolas De Coster	
	Frédéric Demars	
	Olivier Devolder	
	Sébastien Mahaut	
	Benoit Medaets	
	Didier Moës	
	Dominique Offergeld	

Qu'a mis ORES en œuvre pour se conformer au RGPD ?

Chez ORES, nous sommes particulièrement soucieux du respect des droits et libertés de nos clients et de nos employés, ainsi que des autres parties prenantes (personnes physiques) auxquelles nous avons à faire.

La conformité au RGPD est de ce fait un souci constant qui se traduit par les éléments suivants :

- **Gouvernance** :

La mise en conformité d'ORES est passée par la désignation d'un Data Protection Officer au sein du service juridique et par la création d'une équipe de coordination composée de SPOCS, actifs dans les différentes Directions.

Dans l'état actuel de l'organisation d'ORES, les aspects liés à la mission de contrôle des obligations RGPD restent confiés à l'audit interne et aux différents acteurs chargés du contrôle permanent. L'établissement d'un plan de contrôle spécifique « RGPD » où un rôle spécifique serait confié au DPO sera régulièrement réexaminé. Dans ces matières, le DPO a un rôle d'information et de conseil.

Le DPO, lorsqu'il l'estime opportun, bénéficie d'un accès direct aux différentes Directions d'ORES, ainsi qu'à son CEO.

L'accent est mis sur la collaboration continue entre le DPO, le CISO et les SPOCS.

- **Communication et sensibilisation des membres du personnel et de la direction** :

Différentes initiatives sont régulièrement prises depuis 2017 pour faire monter en maturité les collaborateurs au sein des différentes Directions et pour leur apporter la compréhension de la réglementation, nécessaire à la bonne exécution de leurs tâches et ainsi assister les clients dans le cadre de l'exercice de leurs droits.

Des communications récurrentes et ciblées, des présentations adaptées, des FAQ et un espace dédié sur l'intranet ont été mis en place dans un but de formation et d'information constante.

Une bibliothèque est disponible sur l'espace intranet dédié via ce lien :
https://oresonline.sharepoint.com/sites/RGPDCorner.

- **Transparence et « *notice de vie privée* »** :

ORES a publié deux notices de vie privée, l'une à destination de ses clients et l'autre à destination de ses employés.

Le but de ces notices est d'informer les personnes concernées sur les données qui sont traitées par ORES : pour quelles raisons ces données sont traitées, combien de temps et où celles-ci sont conservées et comment les personnes concernées peuvent exercer leurs droits.

ORES dispose également d'une Cookies Policy qui informe de manière complète les visiteurs de notre site sur l'utilisation des cookies et permet à ceux-ci de moduler leur utilisation.

D'autre part, des communications ad hoc sont prévues, lorsque c'est opportun. Une page web est notamment dédiée au compteur communicant.

- **Procédure en cas de violation de données à caractère personnel** :

Une procédure de réponse aux incidents a été décrite. Celle-ci a pour but d'établir une bonne coordination entre le DPO et le CISO pour la mise en place rapide des actions : actions conservatoires et correctrices nécessaires, notification vers l'Autorité de Protection des Données (APD) – dans les 72 heures – et communication adaptée vers les personnes concernées dans les cas où le RGPD l'exige.

Lorsqu'une violation de données à caractère personnel est suspectée par le DPO, ce dernier informera sans délai le Directeur de la Direction concernée, ainsi que le Directeur Corporate. Le DPO émettra une recommandation concernant la notification ou la non-notification de l'incident à l'APD ainsi que la notification ou non-notification aux personnes concernées.

Les décisions relatives à la notification de ces violations et aux mesures éventuelles de publicité seront prises par ces derniers sur la base de la recommandation du DPO qui exécutera les formalités décidées.

Dans le cas où la violation concerne la Direction Corporate, la décision de notification sera prise conjointement par le Directeur Corporate et le Président du Comité de direction.

Si la décision de non (notification) s'éloigne de la recommandation du DPO ou s'il n'est pas possible de dégager une position conjointe des deux Directeurs, dans tous les cas, la responsabilité en sera prise par le Comité de direction.

La procédure et les documents permettant l'évaluation objective de l'impact des violations sont disponibles sur l'espace intranet dédié au RGPD.

- **Droits des personnes** :

La parution des « *notices de vie privée* » couvre l'exigence en matière de droit à l'information.

Un processus interne de réponses aux demandes et plaintes des clients et des membres du personnel concernant les autres droits (particulièrement le droit d'accès) a été établi. Ce processus a pour vocation de permettre aux clients d'exercer facilement leurs droits. Ce processus est basé sur une collaboration avec les SPOCS des différentes Directions, chacun étant responsable de la récolte des informations dans son champ d'action.

Outre les limites habituelles (nécessité de traiter et obligations légales), le droit de rectification des clients peut aussi être limité par la réalité du marché (par exemple impossibilité pour le GRD de corriger les données du registre d'accès sans l'intervention des fournisseurs).

- **« Data Protection by design », « Data Protection by default », DPIA (Analyse d'impact relative à la protection des données)** :

Une procédure unique pour l'évaluation « Security et Data Protection by design » a été rédigée et publiée pour faire écho aux besoins en matière de sécurité des données et des systèmes en général et des besoins spécifiques liés au RGPD en particulier. Concernant toutes les nouvelles initiatives menées dans l'entreprise, une procédure unique a été établie, tant pour les projets que pour les Demandes de Modifications Evolutives.

Cette dernière fournit notamment les éléments nécessaires à la préanalyse (« Questionnaire préalable ») permettant de déterminer si un DPIA doit être mené et fait le lien avec l'outil « PIA » développé par la CNIL[1] qu'ORES a choisi comme outil d'analyse. Le questionnaire préalable constitue également un élément précieux de documentation (data protection dès la conception/principe d'accountability).

Plusieurs DPIAS sur les processus existants ont été menés dans les différentes Directions dans un but de mettre ces processus en conformité.

- **Registre des traitements** :

Un registre des traitements a été établi pour ORES.

Celui-ci permet de recenser les traitements de données et de disposer d'une vue d'ensemble de ce qu'ORES fait avec les données à caractère personnel. Le registre des traitements d'ORES contient tous les champs rendus obligatoires par l'article 30 du RGPD et il participe ainsi à la documentation de la conformité.

La granularité du registre a été validée par le Comité de direction.

Les Directions portent la responsabilité de la mise à jour constante de ce registre et elles bénéficient du soutien du DPO dans cette tâche.

ORES a fait l'acquisition d'un outil « Omniprivacy » dans le but d'en faciliter la tenue à jour.

- **Rétention des données** :

Des efforts sont actuellement menés pour établir la gouvernance en matière de rétention des données en général et des données à caractère personnel en particulier.

Des efforts sont également menés en termes d'archivage (et de digitalisation permettant une meilleure maîtrise des procédures de nettoyage).

Cette mission est confiée à la Direction « Stratégie et Transformation », le DPO apportant son plein concours dans l'analyse des éléments propres au RGPD.

- **Sécurité, Anonymisation / Pseudonymisation** :

Des mesures techniques et organisationnelles ont été établies pour renforcer la sécurité des données à caractère personnel tout au long du cycle de traitement de celles-ci. L'outil d'analyse de risque Ebios a été choisi pour l'évaluation de la robustesse de ces mesures.

ORES s'est engagé dans un trajet de certification ISO 27001. De nombreuses analyses de risques de sécurité ont été menées sur les différents processus de l'entreprise. Les aspects liés aux risques sur les données y sont abordés.

Des efforts ont été initiés en matière de pseudonymisation des environnements de test. ORES reconnait que cet effort doit se poursuivre au travers des futurs projets de transformation (particulièrement Neo).

Engagement

Chez ORES, nous sommes pleinement engagés dans l'application quotidienne du RGPD et nous continuerons d'apporter les modifications nécessaires pour nous conformer à la réglementation, tout en garantissant l'intérêt de l'entreprise et par là de l'ensemble des utilisateurs du réseau.

Nous nous engageons à soutenir et former nos collaborateurs dans le respect des droits de nos clients avec l'ambition de garantir nos standards de services de qualité.

Nous nous engageons à poursuivre nos efforts en matière de rétention et archivage ainsi que de pseudonymisation des données.

[1] Commission Nationale Informatique et Libertés

Nous confions au DPO la mission de nous conseiller en toute indépendance par rapport aux différentes Directions et au mieux de l'intérêt des personnes concernées. Dans son rôle de conseiller, le DPO sera particulièrement attentif à maintenir un niveau d'exigence en ligne avec l'intérêt d'ORES.

Nous nous engageons à informer en temps utile le DPO de tout incident et de tout risque en lien avec la protection des données à caractère personnel dont ORES est le responsable du traitement ou le sous-traitant.

Les décisions de ne pas suivre ses recommandations seront motivées, documentées et conservées.