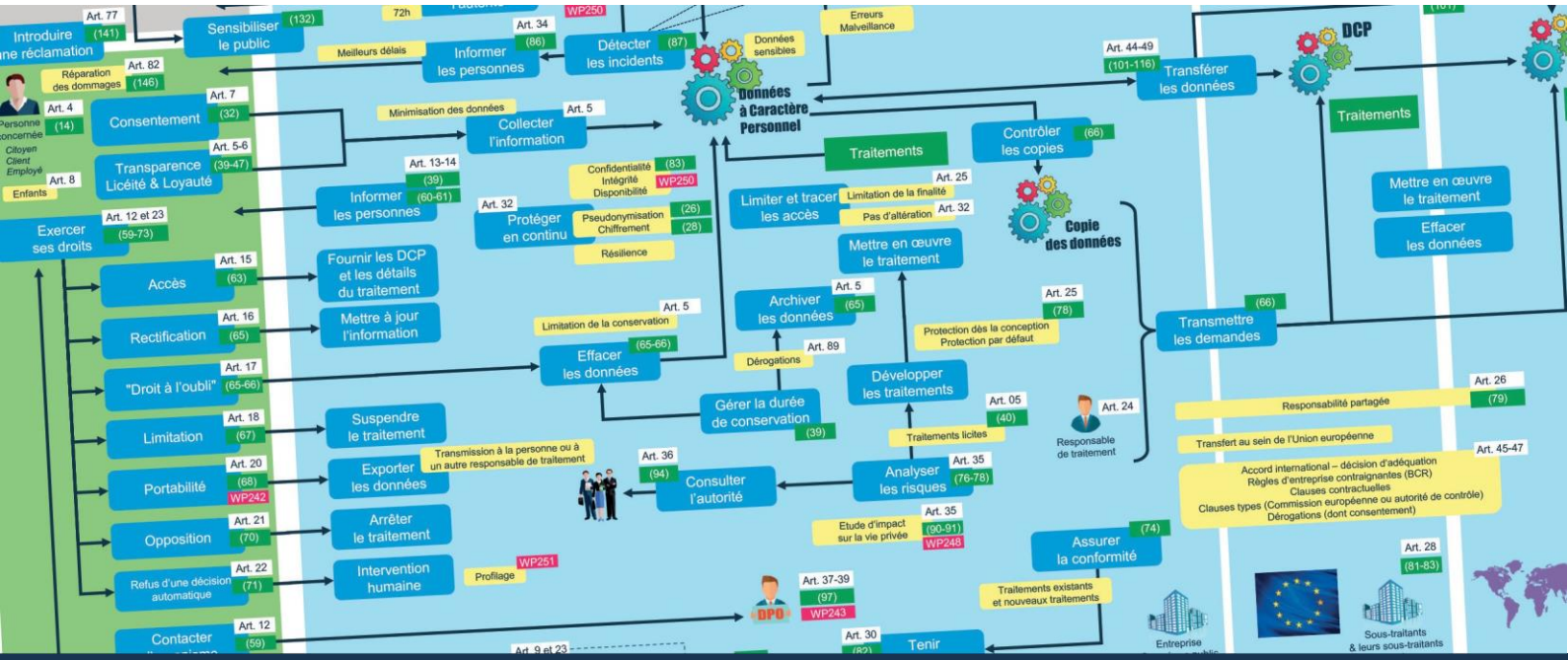
LES FICHES PRATIQUES du CLUSIF - RGPD



OBLIGATIONS DU RESPONSABLE DE TRAITEMENT

Le chapitre IV intitulé « responsable de traitement et sous-traitant » du RGPD régit l'essentiel des obligations qui pèsent sur un Responsable de Traitement (RT) ou un sous-traitant (ST). Il recense ses obligations générales (section 1), celles liées à la sécurité des données personnelles (section 2), aux analyses d'impact sur la protection des données (section 3), à la désignation et aux conditions d'exercice de l'activité du DPO[1] (section 4) et enfin les obligations dans le cadre des codes de conduite et certification.

S'en tenir au seul chapitre IV pour recenser les obligations du RT serait une erreur. En effet, on trouve un peu partout dans le règlement les obligations qu'il doit respecter. Le tableau ci-après synthétise ces obligations.

[1] L'acronyme DPO (Data Privacy Officer) est utilisé pour désigner le délégué à la protection des données (DPD).

Nature de l'obligation	Détail de l'obligation	Observations
Obligations générales		
Responsabilité du RT (*RGPD, Art. 24*)	Obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au Règlement.	Principe de responsabilisation / documentation (*accountability*)
Protection des données dès la conception (*privacy by design*) (*RGPD, Art. 25.1*)	Obligation de mettre en œuvre dès la conception du traitement, des mesures pour protéger les données et les droits des personnes.	Mesures techniques (ex. pseudonymisation) et organisationnelles (ex. minimisation)
Protection des données par défaut (Privacy by default) (*RGPD, Art. 25.2*)	Obligation de mettre en œuvre des mesures garantissant que, par défaut, seules sont traitées les données personnelles nécessaires à chaque finalité.	Application à la quantité de données collectées, à l'étendue de leur traitement, à leur durée de conservation, à leur accessibilité...
Représentants des RT qui ne sont pas établis dans l'UE (*RGPD, Art. 27)*	Lorsqu'il n'est pas établi dans l'UE, le responsable de traitement doit désigner un représentant dans l'UE. Cette obligation ne s'applique ni à une autorité ou un organisme public ni dans les cas de traitement occasionnel ou sans risque majeur.	Cette désignation doit prendre la forme d'un mandat écrit (*C80*).
Traitement effectué sous l'autorité du RT (*RGPD, Art. 29*)	Obligation de donner des instructions pour le traitement des données personnelles aux sous-traitants et aux personnes agissant sous son autorité.	
ST (*RGPD, Art.28*)	Obligation de faire appel à des sous-traitants qui présentent des garanties suffisantes pour la protection des droits de la personne concernée *(Art. 28.1)* Obligation de formaliser le recours à la sous-traitance de second niveau, par une autorisation écrite *(Art. 28.2)* Obligation de formaliser certaines exigences auprès du sous-traitant *(Art. 28.3)*	Guide du sous-traitant de la CNIL[2].
Coopération avec l'autorité de contrôle (*RGPD, Art.31*)	Obligation de coopération avec l'autorité de contrôle.	
Registre des activités de traitement (*RGPD, Art.30*)	Obligation de tenir un registre des traitements dans les cas suivants : - organisation de 250 employés et plus ; - traitement susceptible de comporter un risque pour les droits et libertés des personnes concernées ; - traitement non occasionnel ; - traitement portant sur des données sensibles ou bien relatives à des condamnations pénales et à des infractions.	La tenue d'un registre par toute structure semble une bonne pratique. (voir Position Paper du G29 le 19/04 sur l'article 30.5)
Obligations en matière de sécurité des données personnelles		
Sécurité du traitement (*RGPD, Art.32*)	Le responsable de traitement met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Pour cela, il tient compte de l'état des connaissances, des coûts de mise en œuvre, de la nature, la portée, du	Obligation générale de sécurité L'article 32 énumère une série de mesures à prendre en compte, selon les besoins de l'organisation considérée.

[2] https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Nature de l'obligation	Détail de l'obligation	Observations
	contexte et des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes concernées par le traitement. Les risques sur les données à prendre en compte sont notamment les suivants : destruction, perte, altération, divulgation non autorisée, accès non autorisé, de manière illicite ou accidentelle.	
Violation de données à caractère personnel Notification à l'autorité de contrôle. (*RGPD, Art. 33*)	Obligation de notifier à l'autorité de contrôle les violations de données personnelles qui engendrent un risque pour les droits et libertés des personnes concernées par le traitement. La notification doit intervenir dans les meilleurs délais, si possible 72 heures au plus tard après en avoir pris connaissance. Le responsable de traitement doit justifier des motifs du retard au-delà de ce délai. Obligation de documenter toute violation de données personnelles. La documentation, tenue à disposition de l'autorité de contrôle comprend les informations suivantes : faits concernant la violation, effets de la violation et mesures prises pour y remédier.	Importance de la qualification de la violation de données personnelles, afin de déterminer si la notification doit avoir lieu. Il est vivement conseillé de bien documenter la décision de ne pas notifier. L'obligation de documentation concerne toutes les violations de données personnelles (y compris donc celles qui n'ont pas été notifiées).
Violation de données à caractère personnel Communication aux personnes concernées (*RGPD, Art. 34*)	Le RT doit informer les personnes concernées dans les meilleurs délais, en cas de violations susceptibles d'engendrer un risque élevé pour leurs droits et libertés. Le responsable de traitement est dispensé de cette information : - s'il a mis en œuvre les mesures de protection techniques et organisationnelles appropriées (notamment s'il a chiffré les données de façon à les rendre incompréhensibles), - s'il a pris des mesures ultérieures qui garantissent que le risque élevé n'est plus susceptible de se matérialiser. La communication publique ou une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace est admise au cas où l'information exigerait des efforts disproportionnés.	Rôle déterminant de la CNIL qui peut imposer la communication aux personnes ou bien considérer que la violation de données personnelles entre dans les cas de dispense de communication.

Nature de l'obligation	Détail de l'obligation	Observations
Analyse d'impact relative à la protection des données (PIA) [3]		
PIA (*RGPD, Art. 35*)	Obligation du RT d'effectuer un PIA quand le traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de sa nature, sa portée, son contexte et de ses finalités, *est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*. Le PIA est réalisé avant la mise en œuvre du traitement. Obligation du RT de demander conseil au DPO, s'il a été désigné. Le PIA est obligatoire dans les 3 cas suivants : - Évaluation systématique et approfondie d'aspects personnels concernant les personnes, fondée sur un traitement automatisé, y compris le profilage et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard de la personne ou l'affectant significativement de manière similaire ; - Traitement à grande échelle de données sensibles (particulières, selon la terminologie RGPD) ou de données personnelles relatives aux condamnations pénales et infractions ; - Surveillance systématique à grande échelle d'une zone accessible au public.	Importance de la qualification : seuls les traitements susceptibles d'engendrer un risque élevé sont concernés. En cas de doute, il est toutefois conseillé de réaliser un PIA. Se reporter à la fiche dédiée de cette FAQ et aux lignes directrices du G29. Le RGPD prévoit qu'une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.
Consultation préalable (de l'autorité de contrôle) (*RGPD, Art. 36*)	Consultation obligatoire et préalable à la mise en œuvre du traitement, de l'autorité de contrôle si le PIA révèle que le traitement présente un risque résiduel élevé (interprétation du G29).	Le RGPD énumère les informations qui doivent être fournies à la CNIL. Le PIA fait partie des documents à communiquer.
Délégué à la protection des données (DPO)		
Désignation du délégué à la protection des données (*RGPD, Art. 37*)	Obligation de désigner un délégué dans les cas suivants : - le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ; - les activités de base du RT ou du ST consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; - les activités de base du RT ou du ST consistent en un traitement à grande échelle de catégories particulières (données sensibles) et de données à caractère personnel relatives à des condamnations pénales et à des infractions.	

[3] L'acronyme « PIA » est utilisé indifféremment pour désigner *Privacy Impact Assessment*, étude d'impact sur la vie privée (EIVP), analyse d'impact relative à la protection des données (AIPD) ou encore *Data Protection Impact Assessment* (DPIA).

Nature de l'obligation	Détail de l'obligation	Observations
Codes de conduite et certification		
Codes de conduite (*RGPD, Art. 40*)	Obligation de se conformer aux codes de conduite qui auraient été rendus d'application générale au sein de l'Union par la Commission, par voie d'actes d'exécution.	La mise en œuvre des codes de conduite qui n'ont pas de caractère obligatoire est néanmoins recommandée. Elle est notamment utile lors de la réalisation d'un PIA.
Certification (*RGPD, Art. 42*)	Le RT qui décide de soumettre un traitement au mécanisme de certification doit fournir à l'organisme de certification, voire à l'autorité de contrôle toutes les informations et l'accès à ses activités de traitement, nécessaires pour mener la procédure de certification.	Les certifications, labels et marques en matière de protection des données aident les RT à démontrer que leurs traitements respectent le règlement. Elles ne diminuent toutefois pas leur responsabilité quant au respect du RGPD.
Transferts de données personnelles vers des pays tiers ou à des organisations internationales[4]		
Demande d'autorisation à l'autorité de contrôle (*RGPD, Art. 44 à 50*)	Le RT doit demander son autorisation à l'autorité de contrôle : - pour le transfert des données hors UE, en présence de clauses contractuelles conclues par le RT avec un autre RT, un sous-traitant ou le destinataire des données personnelles dans le pays tiers ; - pour les dispositions à intégrer dans des arrangements administratifs entre autorités publiques ou organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées par les traitements.	La demande d'autorisation n'est pas nécessaire dans le cadre de transferts : - réalisés au sein de l'UE ; - fondés sur une décision d'adéquation de la Commission européenne (i.e. niveau de protection adéquat du pays tiers) ; - disposant de garanties appropriées (règles d'entreprise contraignantes [*BCR*], clauses contractuelles types approuvées par la Commission ou une autorité de contrôle, code de conduite approuvé, mécanisme de certification approuvé…) ; - bénéficiant de dérogations pour des situations particulières (consentement explicite, exécution d'un contrat…). Se reporter également à la fiche dédiée de cette FAQ.
Autres obligations essentielles		
Respect des conditions de licéité du traitement (*RGPD, Art. 5 et 6*)	Obligation du RT de veiller au respect des principes relatifs au traitement des données personnelles (traitement licite, loyal et transparent vis-à-vis des personnes, limitation des finalités, minimisation des données, exactitude, limitation de la durée de conservation, intégrité et confidentialité). Il doit être en mesure de démontrer le respect de ces conditions.	Se reporter également à la fiche dédiée de cette FAQ et au document du G29[5]. Le RT doit tenir compte, pour apprécier la compatibilité des finalités (initiale – secondaire) d'un certain nombre d'éléments (nature des données, existence de garanties appropriées, conséquences possibles du traitement ultérieur pour les personnes concernées …) énumérés par l'article 6 §4.

[4] https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

[5] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Nature de l'obligation	Détail de l'obligation	Observations
Consentement (*RGPD, Art. 7*)	Si le traitement repose sur le consentement (base légale), le RT doit être en mesure de démontrer le recueil du consentement des personnes concernées.	Se reporter également à la fiche dédiée de cette FAQ et au document du G29[6]. Attention à bien respecter le formalisme exigeant de l'article 7 et à prévoir de conserver la preuve de ces consentements pendant la durée du traitement.
Données particulières (« sensibles ») (*RGPD, Art. 9*)	Obligation du RT de ne pas collecter de données interdites (celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, convictions religieuses, l'appartenance syndicales, données de santé …), sauf exceptions (principalement fondée sur le consentement des personnes) énumérées à l'article 9.	Se reporter également à la fiche dédiée de cette FAQ.
Droits des personnes		
Information des personnes Transparence des informations et des communications (*RGPD, Art. 12 à 23*)	Le RT prend des mesures appropriées pour fournir toute information requise dans les cas de collecte directe / indirecte et pour procéder à toute communication en cas d'exercice par les personnes de leurs droits. L'information sur le traitement doit être concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Le RT facilite l'exercice des droits conférés à la personne concernée par les traitements. Il respecte à cet égard la procédure prévue par le RGPD.	Se reporter également à la fiche dédiée de cette FAQ.

[6] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051