Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Berne, le 4 septembre 2018

Note explicative relative à l'obligation de notifier une violation de données à caractère personnel en vertu de l'art. 33 du Règlement (UE) 2016/679 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 (RGPD)

Cette note a pour but d'examiner à l'attention des entreprises établies en Suisse et assujetties au RGDP si l'obligation de notifier une violation des données à caractère personnel à une autorité de contrôle compétente d'un Etat membre de l'Union européenne est susceptible de constituer une infraction au sens de l'art. 271, ch. 1, du code pénal (CP) et si elle nécessite une autorisation de la part de la Confédération.

En vertu de son art. 3, par. 1, le RGPD s'applique principalement au traitement des données à caractère personnel effectué dans le cadre d'activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union européenne, que le traitement ait lieu ou non dans l'Union européenne.

Le RGPD a également une portée extraterritoriale. L'art. 3, par. 2, prescrit en effet que le RGPD s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union européenne par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes dans l'Union européenne (let. a) ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne (let. b).

L'art. 3, par. 2, RGPD a pour conséquence qu'un responsable du traitement ou un sous-traitant établi en Suisse et qui traite des données personnelles concernant des personnes qui se trouvent sur le territoire de l'Union européenne dans le cadre d'une activité au sens de l'art. 3, par. 2, let. a ou b, doit non seulement respecter les prescriptions du RGPD mais est également soumis à la surveillance de l'autorité de contrôle de protection des données compétente (art. 4, ch. 22, et art. 55 RGPD).

L'art. 33 par. 1 RGPD prescrit qu'en cas de violation de données personnelles, le responsable du traitement doit le notifier à l'autorité de contrôle compétente à certaines conditions. En vertu du par. 3, la notification doit au moins indiquer la nature de la violation des données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel, les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues, les conséquences probables de la violation de données ainsi que les mesures prises pour remédier à la situation. Par contre, le catalogue minimum du par. 3 ne prévoit pas que la notification doit indiquer l'identité des personnes concernées. La violation de l'obligation

prévue à l'art. 33, par. 1, RGPD est sanctionnée. L'autorité de contrôle peut en effet prononcer contre le responsable du traitement une amende conformément à l'art. 83, par. 4, let. a, RGPD.

L'art. 271, ch .1, CP punit celui qui, sans y être autorisé, aura procédé sur le territoire suisse, pour un Etat étranger, à des actes qui relèvent des pouvoirs publics ou qui aura favorisé de tels actes.

Selon la doctrine et la jurisprudence, on entend par « actes relevant des pouvoirs publics au sens de l'art. 271, ch. 1, CP » des procédés qui, par leur nature – sans qu'un fonctionnaire y ait pris part – sont de la compétence d'un magistrat ou d'un fonctionnaire. L'applicabilité de l'art. 271, ch. 1, CP ne dépend pas des caractéristiques de l'auteur mais de la question de savoir si l'acte relève des pouvoirs publics. Le bien protégé est la sphère d'influence étatique. Il s'agit de préserver l'inviolabilité du territoire et la souveraineté de l'Etat. L'objet de l'attaque est la souveraineté de la Suisse, c'est-à-dire son droit à ce que des actes étatiques ne soient effectués sur son territoire que par ses propres institutions, à moins qu'une norme n'y autorise une autorité étrangère (p. ex. loi, traité international, ou autorisation accordée par une autorité suisse). Enfin, l'art. 271, ch. 1, CP ne punit pas seulement celui qui accomplit un acte officiel sur sol suisse mais aussi celui qui aura favorisé de tels actes.

De l'avis du Département fédéral de justice et police (DFJP), une notification au sens l'art. 33 RGPD et contenant les informations prévues à l'art. 33, par. 3, ne constitue pas une atteinte à la souveraineté de la Suisse. En effet, Les notifications prévues par l'art. 33 RGPD ne relèvent pas exclusivement, selon les conceptions du droit suisse, de la compétence d'une autorité ou d'un fonctionnaire. Elles ne constituent donc pas un acte relevant des pouvoirs publics au sens de l'art. 271, ch. 1, CP. De plus, l'art. 33 par. 1 RGPD fonde une simple obligation de notifier qui ne s'identifie pas non plus à un tel acte effectué par une autorité étrangère sur le territoire suisse. A défaut d'infraction principale, les notifications prévues par l'art. 33 RGPD ne peuvent dès lors pas non plus constituer une favorisation d'un acte exécuté sans droit pour un Etat étranger.

Au vu de ce qui précède, le DFJP considère que les responsables du traitement établis en Suisse et tombant dans le champ d'application du RGPD en vertu de son art. 3, par. 2, n'ont pas besoin d'obtenir une autorisation de la part de la Confédération au sens de l'art. 31 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration[1] pour notifier une violation des données personnelles à l'autorité de contrôle compétente d'un Etat membre de l'Union européenne.

[1] RS **172.010.1**