Une annonce (très) rapide d'une fuite de données ou une amende salée

Célian Hirsch, le 22 novembre 2021

Le responsable du traitement qui est raisonnablement certain qu'une violation de données a eu lieu doit annoncer la violation à l'autorité compétente dans un délai de 72 heures. Il ne peut pas procéder à des investigations internes avant d'effectuer l'annonce.

Autoriteit Persoonsgegevens, Booking.com, 10.12.2020

EUR 475'000.- d'amende pour 22 jours de retard, soit EUR 21'590.- par jour. C'est le montant dont a dû s'acquitter Booking auprès de l'*Autoriteit Persoonsgegevens* (l'autorité néerlandaise de protection des données) pour n'avoir pas annoncé une fuite de données dans de meilleurs délais (art. 33 par. 1 RGPD).

Le lecteur pourrait ne pas s'offusquer. Après tout, 22 jours de retard, c'est un laps de temps important pour une fuite de données, laquelle doit être annoncée en principe dans les 72 heures. Cela étant, la durée effective du « retard » n'est pas aussi limpide. En effet, le *dies a quo* du délai d'annonce de la fuite est sujet à interprétation, en particulier lorsque la fuite des données n'est pas évidente, ce que nous verrons ci-dessous.

Booking propose une plateforme de réservation d'hébergements en ligne. Ses prestataires – principalement des hôtels – bénéficient d'un accès à l'extranet de Booking afin de pouvoir consulter les détails des réservations effectuées par les clients. L'accès à cet extranet est sécurisé par une authentification à double facteur.

Booking dispose d'une directive interne qui prévoit que tout incident de sécurité doit immédiatement être communiqué à la *Security Team*, notamment s'il est notifié par un prestataire tiers.

Le 9 janvier 2019, un hôtel partenaire de Booking informe la plateforme qu'un client s'est plaint du fait qu'un tiers, prétendant travailler pour l'hôtel, l'aurait contacté afin d'obtenir ses données de carte de crédit.

Le 13 janvier 2019, le même hôtel informe Booking qu'il a reçu une plainte semblable d'un autre client. L'objet du courriel précise « *[External Fraud] / Leaked Guest Information* » et il

débute par « *URGENT* ».

Le 20 janvier 2019, le même hôtel informe Booking d'une troisième plainte. Le même jour, un autre hôtel prévient la plateforme d'un problème semble, avec comme objet « *SECURITY BREACH* ».

Le 31 janvier 2019, la *Security Team* de Booking est informée de l'incident.

Le 4 février 2019, l'équipe de sécurité termine son investigation initiale et informe la *Privacy Team*. Elle informe également toutes les personnes concernées par la fuite.

Le 7 février 2019, la *Privacy Team* de Booking notifie l'incident à l'autorité néerlandaise de protection des données.

L'autorité doit ainsi déterminer le *dies a quo* du délai pour annoncer la fuite des données.

Selon l'art. 33 par. 1 RGPD, le responsable du traitement doit notifier la violation de données à l'autorité de contrôle compétente « 72 heures au plus tard après en avoir pris connaissance ». Le délai commence ainsi à courir avec la prise de connaissance. Mais que signifie « prendre connaissance » de la fuite des données (*having become aware of it* ; *die Verletzung bekannt wurde*) ?

Selon le G29, « un responsable du traitement devrait être considéré comme ayant pris ‹ connaissance › lorsqu'il est raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données à caractère personnel » (G29, Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679, 6 février 2018, p. 11).

En l'espèce, l'autorité considère que le courriel du 13 janvier 2019 (soit le deuxième relatif à l'incident) aurait dû permettre à Booking d'arriver à la conclusion qu'un incident de sécurité s'était produit. En particulier, l'hôtel expéditeur du courriel était déjà arrivé à cette conclusion. Cela ressortait par ailleurs de manière évidente de l'objet du courriel (« *[External Fraud] / Leaked Guest Information* »). La *Security Team* de Booking aurait ainsi dû être immédiatement informée de cet incident le 13 janvier, conformément à la directive interne. Au surplus, le courriel du 20 janvier 2019 était également clair quant à la survenance d'une fuite des données. Cela étant, ce n'est que le 31 janvier que l'équipe de sécurité a finalement été informée de la fuite des données.

Au vu de ces éléments, l'autorité néerlandaise considère que Booking est réputée avoir pris connaissance de la violation de données lors de la réception du courriel du 13 janvier 2019. À cette date, la société disposait de suffisamment d'éléments lui permettant d'être raisonnablement certaine qu'un incident de sécurité s'était produit et que cet incident avait compromis des données personnelles.

Pour sa défense, Booking invoque notamment que la fuite ne trouve pas son origine auprès de sa propre infrastructure. Cela étant, l'autorité considère que la plateforme de réservation en ligne est bel et bien responsable du traitement de l'extranet. Dès lors que la violation de données a eu lieu à partir de l'extranet, Booking est responsable d'annoncer auprès de l'autorité compétente la fuite des données.

Par ailleurs, le fait que Booking se soit engagé à dédommager toutes les personnes victimes de la fuite des données ne change rien à son devoir d'annoncer. En effet, celui-ci est toujours dû par le responsable du traitement, sauf si la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes concernées (art. 33 par. 1 RGPD). Or, en l'espèce, le risque s'est déjà concrétisé puisqu'un tiers a eu accès de manière non autorisée à des données personnelles.

En outre, Booking prétend qu'il était justifié de prendre le temps afin de préparer une seule notification concernant les divers courriels reçus, ce qu'a fait sa *Privacy Team*, plutôt que de notifier séparément chaque violation. Enfin, selon la société néerlandaise, il serait déraisonnable et irréaliste d'un point de vue de la charge administrative et financière d'exiger du responsable du traitement qu'il investigue chaque potentiel incident de sécurité afin de pouvoir annoncer l'éventuelle violation de données dans les 72 heures.

L'autorité néerlandaise admet qu'une enquête, afin de déterminer l'étendue de la fuite, peut prendre plus que 72 heures. Cela étant, un tel examen préliminaire n'est pas nécessaire lorsque le responsable du traitement est déjà raisonnablement certain qu'un incident de sécurité s'est produit et que celui-ci a compromis des données à caractère personnel. Or tel était le cas en l'espèce, lors de la réception du deuxième courriel. Les investigations subséquentes ne permettaient ainsi pas de justifier une annonce tardive.

Concernant la charge administrative et financière, l'art. 32 RGPD impose au responsable du traitement de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Le considérant 87 précise que le responsable du traitement doit en particulier adapter de telles mesures afin de pouvoir établir immédiatement si une violation de données s'est produite. En l'espèce, Booking a précisément

adopté une directive interne et une directive nommée « *Data Incident Response Policy* » afin que l'équipe de sécurité soit informée des éventuels incidents. Le fait que cette démarche n'ait pas été respectée en l'espèce ne peut être imputé qu'à l'entreprise elle-même.

Partant, l'autorité constate la violation de l'art. 33 par. 1 RGPD et fixe l'amende à EUR 475'000.-, après une analyse de l'application de l'art. 83 RGPD (conditions générales pour imposer des amendes administratives).

Cette décision n'est pas unique en son genre. En effet, les autorités irlandaise et espagnole ont également sanctionné, dans deux cas distincts, un responsable du traitement pour avoir annoncé tardivement une fuite des données (DPC – Inquiry into University College Dublin (IN-19–7-4) ; AEPD – PS/00179/2020).

Dans le futur droit suisse, l'annonce d'une violation de la sécurité des données devra être effectuée « dans les meilleurs délais » (art. 24 al. 1 nLPD). Contrairement au droit européen, le texte de la loi ne précise pas le point de départ du délai. À notre avis, en raison de l'adoption de cette disposition pour s'aligner sur le droit européen, il convient de considérer que le délai commence également à courir lorsque le responsable du traitement est raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données personnelles.

Cela étant, vu que le délai est plus étendu qu'en droit européen – il n'y a pas de référence aux 72 heures – et que sa violation n'engendre ni de conséquence pénale ni une amende administrative, la question du début du délai en droit suisse déploie moins de conséquences pratiques qu'en droit européen.

Proposition de citation : Célian Hirsch, Une annonce (très) rapide d'une fuite de données ou une amende salée, 22 novembre 2021 *in* www.swissprivacy.law/105