Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

JURISTENDANCES INFORMATIQUE ET LIBERTES

n° 65 – Sept.-Oct. 2015

INVALIDATION DE L'ACCORD SAFE HARBOR

La protection des données transférées de l'Europe vers les Etats-Unis

▪ La Cour de justice de l'Union européenne (CJUE) a estimé, dans une décision du 6 octobre 2015, que le mécanisme d'adéquation du Safe Harbor n'était pas conforme au droit européen.

▪ Dans l'affaire Maximilian Schrems v Data Protection Commissioner (C-362/14) (1), la CJUE a invalidé le Safe Harbor. Elle a en effet estimé que ce mécanisme de protection des données à caractère personnel, auquel les entreprises américaines peuvent adhérer afin de recevoir des données à caractère personnel de pays appartenant à l'Union européenne, ne permettait pas de garantir, de manière effective, un **niveau de protection adéquat** des données à caractère personnel.

▪ Selon la CJUE, les **recours** possibles pour les citoyens européens dont les données sont transférées aux Etats-Unis et qui souhaitent exercer leurs droits sont notamment trop faibles.

▪ De plus, les autorités publiques américaines peuvent accéder massivement et de façon indifférenciée aux données des citoyens européens, sans pour autant assurer une protection juridique efficace.

▪ Sur un plan plus procédural, la décision de la CJUE indique également que les **autorités nationales de protection des données**, par exemple la Cnil, peuvent analyser en toute indépendance les conditions d'un transfert de données vers un pays situé en dehors de l'Union européenne et examiner si ce transfert respecte les dispositions de la directive (2), même si une décision de la Commission européenne reconnait déjà le caractère adéquat de la protection dans ce pays.

L'impact de la décision de la Cour de justice européenne

▪ Suite à l'invalidation de l'accord Safe Harbor, il n'est plus possible de réaliser un transfert de données à destination des Etats-Unis par le biais de l'adhésion au Safe Harbor.

▪ Toutefois, les transferts de données à destination des Etats-Unis pourront toujours être réalisés, par exemple s'ils sont encadrés par :

- des clauses contractuelles types ; ou
- des BCR ou règles d'entreprise.

▪ Les autorités nationales réunies au sein du G29 le 15 octobre 2015 ont demandé aux institutions européennes ainsi qu'aux gouvernements concernés de trouver des solutions juridiques et techniques d'ici 3 mois, soit **jusqu'au 31 janvier 2016** (3). Les autorités nationales se sont également engagées à lancer une **campagne d'information** auprès des entreprises concernées et sur leurs sites respectifs.

▪ La Commission européenne a quant à elle réitéré sa volonté de travailler en coopération avec les autorités américaines pour établir un **Safe Harbor 2.0**. Ce projet, déjà en discussion depuis deux ans, prendra certainement en considération les éléments soulevés dans la décision de la CJUE.

L'enjeu

Le non-respect des règles en matière de transferts en dehors de l'Union peut être sanctionné de 300 000 € d'amende et de 5 ans d'emprisonnement.

(1) CJUE 6-10-2015 Aff. C-362/14 Maximillian Schrems c/ Data Protection Commissioner

(2) Directive 95/46/CE du 24-10-1995.

(3) G29, Communiqué de presse, 6-10-2015.

Les conseils

Etablir une cartographie des flux transfrontières à destination des Etats-Unis et identifier ceux qui sont encadrés par le Safe Harbor.

Etudier les possibilités d'encadrement de ces transferts par des mécanismes alternatifs au Safe Harbor.

CHLOE TORRES

LES COOKIES EXEMPTES PAR LA CNIL DE RECUEIL DU CONSENTEMENT

L'état des lieux

▪ Les cookies ne peuvent être déposés ou lus sur un équipement terminal tant que son **utilisateur**, **préalablement informé**, n'a pas donné son consentement.
▪ Les cookies sont des données stockées dans l'équipement terminal d'un utilisateur et utilisées par le site ou l'application mobile pour envoyer des informations et en recevoir (par exemple un identifiant de session, le choix d'une langue ou une date). L'article 32 II de la loi Informatique et libertés dispose :
« Tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète, sauf s'il l'a été au préalable, par le responsable du traitement ou son représentant :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques, ou à inscrire des informations dans cet équipement ;
- des moyens dont il dispose pour s'y opposer.

Ces accès ou inscriptions ne peuvent avoir lieu qu'à condition que l'abonné ou la personne utilisatrice ait exprimé, après avoir reçu cette information, son accord qui peut résulter de paramètres appropriés de son dispositif de connexion ou de tout autre dispositif placé sous son contrôle.
Ces dispositions ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- soit est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur ».

▪ Les responsables de traitement qui exploitent des cookies doivent informer l'utilisateur et recueillir son consentement préalable. Les éditeurs de sites doivent en outre solliciter le consentement de l'utilisateur tous les **13 mois**, au maximum.

Nouvelle exemption de consentement reconnue par la Cnil

▪ La Cnil avait déjà reconnu que les **cookies Piwik**, qui sont des cookies de mesure d'audience, sous réserve de respecter quelques paramétrages, pouvaient être dispensés du recueil du consentement alors que ceux-ci devaient normalement en relever.
▪ En modifiant son guide des cookies, elle a reconnu la même possibilité pour les **cookies d'AT Internet**, sous réserve de certains paramétrages.
▪ Pour pouvoir bénéficier de cette exception reconnue par la Cnil, l'éditeur du site ou de l'application mobile doit notamment :

- informer les internautes de l'existence des cookies de mesure d'audience,
- implémenter l'option opt-out permettant de refuser les cookies AT internet. Cette solution sera différente selon qu'il s'agit d'un site internet ou d'une application mobile.

▪ Pour aider les éditeurs à mettre en conformité leurs sites ou applications mobiles, l'éditeur AT internet a établi un **guide de mise en conformité** qui est accessible sur le site de la Cnil.

Les enjeux

L'obligation mise à la charge des éditeurs de sites et d'applications mobiles d'assurer l'information des utilisateurs et de recueillir leur consentement est une préoccupation majeure de la Cnil dans le cadre de ses pouvoirs de sanction et de contrôle.

En parallèle, la Cnil leur fournit des outils d'aide à la mise en conformité.

Les conseils

Il est recommandé aux éditeurs de sites et d'applications mobiles de mettre en conformité leurs sites et applications mobiles par la mise en place d'une politique Cookies et d'un module de recueil du consentement adapté aux différents types de cookies utilisés, lorsqu'ils sont soumis au recueil du consentement.

CELINE AVIGNON
ANNE RENARD

LES TRANSFERTS DE DONNEES VERS LES ETATS-UNIS

Comment identifier des flux de données à destination des Etats-Unis ?

Les transferts de données à destination des Etats-Unis sont ceux pour lesquels les destinataires sont situés aux Etats-Unis, tels qu'une filiale ou une maison mère d'un groupe située aux Etats-Unis, un sous-traitant situé aux Etats-Unis, un sous-traitant exportant les données aux Etats-Unis, etc.

Les flux de données à destination des Etats-Unis plus précisément couverts par le Safe Harbor sont ceux dont le destinataire est inscrit sur la liste des entreprises adhérentes au Safe Harbor du Département du Commerce américain.

L'invalidation du Safe Harbor signifie-t-elle que les entreprises européennes ne peuvent plus transférer de données aux Etats-Unis ?

Non. La décision de la CJUE invalide uniquement l'accord Safe Harbor, ce qui signifie que les transferts de données à destination des Etats-Unis ne peuvent plus être couverts par le mécanisme du Safe Harbor.

En revanche, ces transferts peuvent toujours être mis en œuvre s'ils sont encadrés par d'autres mécanismes, tels que des clauses contractuelles types ou des BCR.

Les clauses contractuelles types ou les BCR peuvent-elles être utilisées par tous les responsables de traitement exportant des données aux Etats-Unis ?

Non. Les clauses contractuelles types ou les BCR permettent d'encadrer des transferts selon des critères précis.

Lorsque le transfert de données est effectué au sein d'un groupe, par exemple d'une filiale à une maison mère, le transfert peut-être encadré par des clauses contractuelles types ou des règles d'entreprise (BCR).

Si le transfert n'est pas effectué au sein d'un groupe mais entre deux groupes différents, par exemple, seules des clauses contractuelles types peuvent l'encadrer.

Il existe deux sortes de clauses contractuelles types, en fonction de la qualification du destinataire : les clauses contractuelles types de responsable de traitement à responsable de traitement et les clauses contractuelles types de responsable de traitement à sous-traitant (1).

Référence

((1) Cnil, Guide relatif aux transferts Hors Union européenne.

Prochain petit-déjeuner

Réforme du « Paquet marque » : anticiper pour mieux innover : 4 novembre 2015

▪ Anne-Sophie Cantreau et Virginie Brunot animeront un petit-déjeuner débat dédié à la réforme du droit des marques.

▪ L'adoption de cette réforme se profile à l'horizon 2016 :

- harmonisation renforcée des pratiques nationales ;
- diminution des coûts d'enregistrement ;
- nouvelle définition de la marque afin de prendre en considération les évolutions et usages technologiques ;
- renforcement de la lutte contre la contrefaçon et de la protection du consommateur ;
- simplification des actions en nullité et en déchéance ;

▪ telles sont les principales orientations de la réforme.

▪ En juin dernier, le Conseil de l'Union européenne a approuvé un accord de compromis sur cette réforme qui vise à améliorer « les conditions d'innovation des entreprises » et à renforcer l'efficacité de la protection des marques au sein de l'Union européenne. Cette étape apparaît décisive dans l'adoption d'une réforme appelée à modifier le droit des marques tant au niveau national qu'au niveau européen.

▪ Il apparaît nécessaire pour les acteurs économiques d'anticiper cette refonte pour, dès à présent, adapter leurs pratiques et leur politique de protection, ce qui implique d'aborder les questions suivantes :

- Quels nouveaux signes pourront être protégés ?
- Quelles nouvelles opportunités ? Quelles limites ?
- Quelles précautions prendre pour définir un périmètre de protection efficace ?
- Comment envisager l'introduction d'une marque européenne de certification ?
- Quelles sont les conséquences de la mise en place de procédure en nullité et en déchéance de marque devant les offices de propriété industrielles ?
- Quels nouveaux moyens d'actions pour défendre sa marque ? Sa marque de renommée ?

▪ Telles sont quelques-unes des questions qui seront abordées lors du petit-déjeuner débat.

▪ **Lieu :** de 9h30 à 12h00 (accueil à partir de 9h00) dans nos locaux, 58 bd Gouvion-Saint-Cyr, 75017 Paris.

▪ **Inscription gratuite** (sous réserve des places disponibles).

▪ L'enregistrement en ligne est obligatoire pour y assister : formulaire en ligne

La JTIL est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan.

Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier.

Diffusée uniquement par voie électronique – gratuit – ©Alain Bensoussan 2014

ISSN 1634-0698

Abonnement à partir du site : http://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-juristendance

NOTRE RESEAU DE CORRESPONDANTS ORGANIQUES LEXING VOUS INFORME

European Court of Justice invalidates Safe Harbor for data transfer to the US

Article de Tim Christopher Caesar

Lexing Allemagne

Beiten Burkhardt Rechtsanwaltsgesellschaft mbH

- In its Judgment of 6 October 2015, the ECJ ruled that the Safe Harbor Agreement is not capable of legitimizing data transfer into the US.
- The EU Data Protection Directive – and, by extension, the national German data protection law – allows data transfer into non-European third countries (inter alia, the US) only if an adequate data protection level is guaranteed there. The Safe Harbor Agreement between the EU and the US permits the transfer of personal data from Europe to self-certified entities in the US. However, according to the ECJ ruling, the Safe Harbor Agreement offers no adequate and sufficient protection level for personal data from Europe.
- The Court declared the relevant legitimizing legal act of the EU Commission null and void. Furthermore, the ECJ strengthened once again the independency and competence of data protection supervisory authorities to investigate.
- **Are there alternatives to Safe Harbor?** The ECJ Judgment refers directly only to data transfers which are based on the Safe Harbor principles. Therefore, alternative safeguarding of data transfers is still possible.
- Accordingly, data transfers can still be based in particular on EU standard contract clauses or "Binding Corporate Rules".
- **What is going to happen and what are the next steps?** We expect that, after a reasonable transition period, the supervisory authorities will stop the data transfer based on the Safe Harbor Agreement.
- As long as the decisions of the EU Commission concerning standard contract clauses are not declared void by the ECJ, these standard contract clauses are, in principle, still a suitable instrument for data transfers to the US. However, in the individual case supervisory authorities may prohibit data transfers if the rights of the persons affected are not safeguarded, as also ruled by the ECJ.
- **What has to be done for the time being?**
  - Use the transitional period;
  - Analyze your data transfers to the USA;
  - Ask your provider whether there are alternatives to Safe Harbor which could be implemented at short notice;
  - Group data transfer: If your intra-group data transfer is based on Safe Harbor principles, you should look – in the short term - for alternative safeguarding instruments, e.g. on the basis of standard contract clauses;
  - If required, contact the competent data protection supervisory authority. We could – if requested – in our capacity as advisers committed to professional secrecy coordinate and agree anonymously and legally privileged on facts and approaches with the authorities;
- Do not wait for the Basic Data Protection Regulation. The new EU-wide regulation is likely to come in 2016. However, with regard to the requirements in international data transfer for safeguarding the data protection level, it will hardly involve relief for data-exporting enterprises.

Avis du G29 sur un code de conduite sur le Cloud Computing

▪ Le 22 septembre 2015, le Groupe Article 29 a rendu un avis sur un code de conduite sur le Cloud Computing (1) rédigé par le Cloud Select Industry Group (C-SIG), un groupe composé de représentants du secteur de l'industrie.
▪ Selon le G29, les dispositions du code de conduite proposé ne sont pas toutes conformes à la directive 95/46/CE sur la protection des données à caractère personnel.
▪ Le G29 souligne notamment que le Code pourrait être davantage conforme s'il donnait dans une annexe des informations relatives aux données traitées, telles que le lieu du traitement, si des données sensibles sont traitées, les mesures de sécurité mises en œuvre, les exigences en matière de flux transfrontières, la possibilité de mener des audits, le droit des utilisateurs à la portabilité des données, etc.

(1) G29, Avis 02/2015 du 22/09/2015, WP 232

Droit au déréférencement : rejet du recours gracieux formé par Google

▪ La présidente de la Cnil a rejeté le recours gracieux formé par la société Google suite à la mise en demeure dont elle avait fait l'objet en mai 2015.
▪ La société Google a reçu des demandes de citoyens français et a procédé au déréférencement de ces personnes sur les extensions européennes du moteur de recherche, mais non pas sur les autres extensions ou sur google.com.
▪ La Cnil l'a donc mise en demeure de procéder au déréférencement sur tous les noms de domaine de son moteur de recherche.
▪ Fin juillet, Google a formé un recours gracieux au motif que l'injonction contenue dans la mise en demeure entravait le droit à l'information du public.
▪ La Cnil a rejeté ce recours au motif notamment que les extensions géographiques ne sont qu'un chemin d'accès au traitement et que ne pas faire droit à une demande de déréférencement sur toutes les extensions revenait à priver d'effectivité ce droit.
▪ Suite au rejet du recours, Google devra se conformer à la mise en demeure.

Deux nouvelles mesures de simplification dans le secteur de la santé

▪ La Cnil a adopté deux nouvelles mesures de simplification dans le domaine de la santé : l'autorisation unique AU-043 et la méthodologie de référence MR-002.
▪ L'autorisation unique AU-043 est relative aux programmes de dépistage organisé du cancer du sein et du cancer colorectal (2). Elle concerne la constitution de fichiers des personnes éligibles aux programmes aux fins d'invitation aux opérations de dépistage, le suivi des personnes participant aux programmes et la gestion des contacts avec les médecins traitants, les spécialistes et les laboratoires de lecture. Elle s'adresse aux structures de gestion qui assurent une mission de service public d'organisation locale des dépistages organisés des cancers.
▪ La méthodologie de référence MR-002 (3) encadre quant à elle les études non interventionnelles de performances de matière de dispositifs médicaux de diagnostic in vitro. Afin de guider les responsables de traitement concernés, la Cnil a également publié une grille d'analyse spécifique accompagnant la méthodologie MR-002 (4).

(2) Cnil, Délib. 2015-175 du 11-6-2015.

(3) Cnil, Délib. 2015-256 du 16-7-2015.

(4) Grille d'analyse spécifique accompagnant la MR-002.

Formations intra-entreprise : 2e semestre 2015

LE CABINET A LA QUALITE D'ORGANISME DE FORMATION PROFESSIONNELLE DEPUIS 30 ANS.

Informatique et libertés

Informatique et libertés (niveau 1) : Identifier et qualifier les intervenants et les responsabilités, prévenir les risques et cerner les formalités obligatoires.	27-11-2015
Informatique et libertés (niveau 2) : - Approfondir les connaissances de base acquises dans le domaine Informatique et libertés (politique de conformité, etc.).	16-12-2015
Cil (niveau 1) : Permettre au Cil de maîtriser les obligations et responsabilités qui lui incombent et de savoir les mettre en œuvre.	01-12-2015
Informatique et libertés secteur bancaire : Sensibiliser les opérationnels sur les risques Informatique et libertés liés aux traitements du secteur bancaire.	15-10-2015
Informatique et libertés collectivités territoriales : Informer les collectivités territoriales sur les modalités d'application de la réglementation Informatique et libertés.	07-10 et 04-12-2015
Devenir Cil : Mettre en œuvre une politique de protection des données efficace (accountability, etc.) et résoudre les questions complexes (réseaux sociaux, etc.).	10-11-2015
Cil (niveau 2 expert) : Perfectionnement et résolution de questions complexes ; acquisition de méthodologie pour exercer l'activité selon l'approche Privacy by Design.	05-11 et 09-12-2015
Contrôles de la Cnil : Connaître l'étendue des pouvoirs de la Cnil et ses moyens de contrôle, apprendre à dialoguer avec la Cnil (notamment par le biais d'un jeu de rôle).	17-12-2015
Informatique et libertés à l'attention du comité exécutif : Sensibiliser les membres du comité exécutif aux risques Informatique et libertés liés à leur activité.	Selon demande