# Avis relatif à la protection de la vie privée dans le cadre d’activités spécifiques

## Article 13 – Notification RPGD (Règlement général sur la protection des données) concernant les informations personnelles contenues dans les clips (enregistrements vidéo saisis en route)

### Identité, coordonnées et représentant de l’équipementier

L’équipementier est *Mobileye Vision Technologies Ltd*. domicilié au 13, rue Hartom, Jérusalem, 9777513, Israël. Courriel : [privacy@mobileye.com](mailto:privacy@mobileye.com).

Représenté au sein de l’EEE par le groupe affilié *Mobileye Germany GmbH* , domicilié au 21, rue Emanuel-Leutze-Str., 40547 Düsseldorf, Allemagne.

### Collecte des enregistrements vidéos de route

Certains véhicules d’essai mis en œuvre par Mobileye même ou par nos clients, sont équipés de produits prototypes qui, au fur et à mesure que ces véhicules roulent sur la route, collectent et emmagasinent un enregistrement vidéo de l’extérieur du véhicule sous forme d’une série de vidéo-clips de courte durée (« **Clips »**). Naturellement, ces clips contiennent souvent des informations personnelles (« IP », c’est-à-dire des données relatives à une personne physique identifiée ou identifiable, comme une photo du conducteur ou une plaque d’immatriculation du véhicule). Dans le cas de véhicules d’essai mis en œuvre par un client, les clips nous sont communiqués par transfert de fichier sécurisé ou sur disques réels. (Les clients Mobileye peuvent aussi conserver des copies de ces clips enregistrés par l’un des produits Mobileye, à des fins personnelles, internes.)

### Que fait Mobileye des clips ? (‘objectif de traitement’)

Mobileye utilise ces clips pour le développement interne du produit, sa validation, ses essais et la recherche afférente au produit. Plus particulièrement, nous nous en servons pour ‘travailler’ et tester notre technologie ; et essentiellement pour en améliorer la précision d’identification des divers objets rencontrés sur la route. Ainsi, dans la mesure où les clips contiennent des informations IP, Mobileye ne s’y intéresse que sous leur forme générique (à savoir la forme générique ou l’apparence d’un visage ou d’une plaque minéralogique, et non les signes caractéristiques d’un visage en particulier ou d’une plaque d’immatriculation spécifique) de sorte que par exemple, notre technologie puisse devenir encore plus performante dans l’identification de piétons en tant que tels, permettant ainsi de les distinguer du reste du trafic routier.

### Minimisation des infos IP saisies par Mobileye

Mobileye met un point d’honneur à appliquer différentes mesures pour réduire autant que possible le volume net d’infos personnelles (IP) contenues dans les clips, par ex. par compression des données. (Les clips non comprimés sont cependant conservés, mais utilisés seulement pour des essais de simulation afin de tester le code innovateur Mobileye en séquences de ‘vie réelle’ – par exemple, un développeur Mobileye pourrait vouloir tester une innovation dans le domaine de la détection de piétons sur la base d’un grand nombre de clips offrant des scènes de pluie la nuit – situation où les piétons sont bien moins visibles. Dans ce cas, le nouveau code est simplement appliqué aux clips ‘en arrière-plan’ et le développeur ne voit que les résultats.)

### Quel est le fondement légal permettant à Mobileye de collecter et d’utiliser les clips ? (‘légitimité du traitement’)

L’intérêt de Mobileye à collecter et à utiliser les clips est légitime aux fins susmentionnées, à savoir améliorer nos solutions technologiques d’assistance avancée à la conduite et éventuellement mettre en service des véhicules autonomes – objectif porteur d’un avantage social incontestable, celui de considérablement réduire les accidents de la route avec ce que cela implique de morts et de blessés.

### Transfert de clips hors Mobileye (‘types de destinataires des informations personnelles’)

Les clips ne ‘sortent’ de Mobileye que dans quelques cas précis :

1. Si les clips sont stockés à l’aide de tiers processeurs, afin d’exploiter la puissance informatique massive de ces derniers et leur extensibilité en temps réel ; ou
2. Si Mobileye partage un petit nombre de ces clips, *sous format comprimé*, avec des employés hors site en Israël ou des entrepreneurs externes, à fin de marquage (*tagging*), c’est-à-dire si des humains ‘identifient’ certaines caractéristiques d’un clip pour améliorer ou affiner la précision d’identification par le logiciel Mobileye ; ou pour vérification après-coup d’un marquage (identification), c’est-à-dire si des humains inspectent et vérifient la précision d’identification du logiciel Mobileye ; ou
3. Si Mobileye partage un très petit nombre de clips individuels avec des tiers – clients ou partenaires, dans le cadre d’objectifs commerciaux ; ou
4. Si, pour faire la démonstration de la technologie Mobileye, des clips sont mis en ligne sur les différents sites web de Mobileye ou sur des chaînes de réseaux sociaux, ou si des cadres supérieurs de Mobileye les projettent face à un public de clients – existants ou potentiels, au sein d’une entreprise ou lors d’un évènement commercial. Dans tous les cas, le nombre de clips concerné reste minime.

Le transfert de clips aux termes des alinéas ‎(i)-‎(iii) est effectué soit (i) par télétransmission et téléchargement via des services privés et sécurisés tels que des services sans fils évolués (et non via des services internet intermédiaires tels que Dropbox), soit (ii) par l’envoi de disques durs via un service renommé de livraison à l’international tel que FedEx (certains de ces disques étant eux-mêmes sécurisés par cryptage ou protocole similaire).

En cas de transfert de clips vers d’autres pays, Mobileye s’appuie sur une combinaison de décisions d’adéquation de l’Union Européenne et de normes relatives à la protection des données.

### Délai de conservation d’un clip

Mobileye conserve les clips tant qu’ils s’avèrent utiles, eu égard aux objectifs susmentionnés.

### Droits des particuliers quant au respect de leurs informations personnelles (IP) contenues dans un ou plusieurs clip(s)

Les particuliers disposent de divers droits garantis par le RGPD (Règlement général sur la protection des données) quant aux données personnelles les concernant. Toutefois, veuillez noter que ces droits sont nécessairement limités, vu que Mobileye ne collecte ni ne répertorie les IP (il n’existe aucun mécanisme permettant par exemple, une recherche dans la base de données des clips portant sur un ou plusieurs protocole(s) relatif(s) à un quelconque véhicule ou particulier). En conséquence, il est tout à fait improbable que Mobileye puisse identifier un particulier selon la base de données de ses clips, à moins que ce particulier fournisse une information supplémentaire comme le lieu et l’heure auxquels il/elle pense que le ou les clip(s) concerné(s) a/ont été enregistré(s)\*.

Néanmoins, Mobileye considèrera toute demande, au cas par cas.

\* Dans le cas inhabituel où un particulier échangerait une observation avec le conducteur d’un véhicule d’essai mis en œuvre par Mobileye, en temps réel ou presque réel, les conducteurs ont alors l’instruction d’enregistrer ces observations et de nous les faire suivre pour inspection. Dans ce seul cas, qui reste exceptionnel, il serait possible, nonobstant l’énoncé ci-dessus, d’identifier et d’effacer le ou les clip(s) en question.

### Droit des particuliers à déposer une plainte

Tout particulier peut déposer une plainte auprès des autorités de surveillance locales. La liste de ces autorités de surveillance (telle qu’elle est vérifiée au jour de la publication de cet avis) est disponible [ici](http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm).

## Article 14 Notification RPGD (Règlement général sur la protection des données) concernant les données des segments routiers enregistrés par les véhicules équipés d’origine (OEM)

### Identité, coordonnées et représentant de l’équipementier

L’équipementier est *Mobileye Vision Technologies Ltd*. domicilié au 13, rue Hartom, Jérusalem, 9777513, Israël, courriel : [privacy@mobileye.com](mailto:privacy@mobileye.com).

Représenté au sein de l’EEE par le groupe affilié *Mobileye Germany GmbH* domicilié au 21, rue Emanuel-Leutze-Str., 40547 Düsseldorf, Allemagne.

### Que sont les données de segment routier (DSR) ?

Certains véhicules collectent et transmettent des données sur leur trajet, que nous appelons ‘données de segment routier’ ou DSR. Les DSR sont une représentation mathématique (séquences ou métadonnées alphanumériques) du paysage de rue, comprenant l’emplacement de divers points de repère routiers statiques, fixes autour du véhicule, comme les feux et panneaux de signalisation, ainsi que des données dynamiques telles que les nids-de-poule, places de parking etc.

Chaque élément des DSR inclut également la date, l’heure et les géo-références (GPS) qui lui correspondent.

### Qu’est-ce qu’un véhicule équipé d’origine (OEM) et quels sont ceux qui collectent des données DSR ?

Un véhicule équipé d’origine (OEM) est un véhicule dans lequel la technologie Mobileye a été intégrée par son fabricant pendant la fabrication (contrairement aux « **Véhicules à dispositif embarqué d’un parc automobile »** qui sont desvéhicules sur lesquels le système embarqué Mobileye 8 Connect™ a été installé après fabrication). Le logiciel fonctionnant sur véhicules équipés d’origine collecte des données DSR suivant certaines itérations de la puce EyeQ® de Mobileye.

Remarque : les données DSR collectées par les véhicules à dispositif embarqué sont font l’objet d’une [notification séparée](#_Article_13_GDPR).

### Les données DSR d’un véhicule équipé d’origine (OEM) contiennent-elles des informations personnelles (« IP » désignant toute information relative à une personne physique identifiée ou identifiable) ?

Le premier à recevoir les données DSR est le fabricant du véhicule OEM en question. Avant de transmettre ces DSR à Mobileye, le fabricant retire les DSR de toute éventuelle IP (y compris pour lui-même), en appliquant pour cela plusieurs ou toutes les façons suivantes : (i) en brouillant l’indentification du véhicule, (ii) en effaçant les DSR correspondant aux toutes premières et toutes dernières minutes du trajet, et (iii) en retirant de chaque trajet un segment proportionnel – par exemple 1 km tous les 10 km.

Ainsi, Mobileye est fermement convaincu que les DSR en provenance des fabricants de véhicules équipés d’origine sont exempts d’IP – Mobileye ne dispose d’aucun moyen qui lui soit propre, pour faire correspondre des données DSR spécifiques au véhicule OEM qui les a collectées. Néanmoins, la présente notification est entièrement établie selon l’hypothèse que les DSR reçues par Mobileye des fabricants de véhicules OEM contiennent malgré tout, des infos IP.

### Que fait Mobileye des données de segment routier (DSR) ? (‘objectif de traitement’)

Mobileye consolide et organise le flux continu des DSR reçues depuis les véhicules pertinents, ce qui conduit à la formation d’une carte virtuelle de haute précision en temps réel, appelée « Roadbook™ » (Guide routier).

### Quel est le fondement légal permettant à Mobileye de collecter et d’utiliser les données DSR ? (‘légitimité du traitement’)

L’intérêt de Mobileye à collecter et à utiliser les données de segment routier (DSR) est légitime, celles-ci représentant un élément essentiel pour un écosystème de routier constitué de véhicules autonomes ou quasi-autonomes. La mise en service de véhicules autonomes est un objectif porteur d’un avantage social incontestable, celui de considérablement réduire les accidents de la route avec ce que cela implique de morts et de blessés.

### Transfert de données DSR hors Mobileye (‘types de destinataires des données IP’)

Mobileye est susceptible de partager des données DSR ‘brutes’ avec, par exemple, des cartographes. De telles données DSR, et *a fortiori*, un Roadbook (Guide routier) dérivé de DSR consolidées et organisées ne contiennent certes aucune information personnelle (IP). En cas de transfert de DSR vers d’autres pays, Mobileye s’appuie sur une combinaison de décisions d’adéquation de l’Union Européenne et de normes relatives à la protection des données.

### Délai de conservation des données DSR

Comme énoncé plus haut, l’utilisation principale des données DSR réside dans leur consolidation et leur organisation en un ‘Roadbook’ (Guide routier). Les données DSR brutes sont toutefois conservées tant qu’elles s’avèrent utiles.

### Droits des particuliers quant au respect de leurs informations personnelles (IP)

Les particuliers disposent de divers droits garantis par le RGPD (Règlement général sur la protection des données) quant aux données personnelles les concernant. Mobileye considèrera, au cas par cas, toute requête d’exercer ces droits.

### Droit des particuliers à déposer une plainte

Tout particulier peut déposer une plainte auprès des autorités de surveillance locales. La liste de ces autorités de surveillance (telle qu’elle est vérifiée au jour de la publication de cet avis) est disponible [ici](http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm).

## Article 13 Notification RPGD (Règlement général sur la protection des données) concernant les informations personnelles (IP) contenues dans les données des segments routiers (DSR) enregistrées par les véhicules à dispositif embarqué d’un parc automobile

### Identité, coordonnées et représentant de l’équipementier

L’équipementier est *Mobileye Vision Technologies Ltd*. domicilié au 13, rue Hartom, Jérusalem, 9777513, Israël, courriel : [privacy@mobileye.com](mailto:privacy@mobileye.com).

Représenté au sein de l’EEE par le groupe affilié *Mobileye Germany GmbH* domicilié au 21, rue Emanuel-Leutze-Str., 40547 Düsseldorf, Allemagne.

### Que sont les données de segment routier (DSR) ?

Certains véhicules collectent et transmettent des données sur leur trajet, que nous appelons ‘données de segment routier’ ou DSR. Les DSR sont une représentation mathématique (séquences ou métadonnées alphanumériques) du paysage de rue, comprenant l’emplacement de divers points de repère routiers statiques, fixes autour du véhicule, comme les feux et panneaux de signalisation, ainsi que des données dynamiques telles que les nids-de-poule, places de parking etc.

Chaque élément des DSR inclut également la date, l’heure et les géo-références (GPS) qui lui correspondent, et en cas de véhicules à dispositif embarqué d’un parc automobile, le numéro de série du système Mobileye qui les a saisies.

### Qu’est qu’un véhicule à dispositif embarqué d’un parc automobile et quels sont ceux qui saisissent les données DSR ?

Un véhicule à dispositif embarqué d’un parc automobile est un véhicule appartenant à la flotte automobile d’une entreprise, sur lequel le système embarqué Mobileye 8 Connect™ a été installé après fabrication (contrairement aux « **véhicules équipés d’origine »** [OEM], dans lesquels la technologie Mobileye a été intégrée par son fabricant pendant la fabrication). Les véhicules à dispositif embarqué d’un parc automobile collectent des données DSR.

Remarques : les données DSR collectées par les véhicules équipés d’origine font l’objet d’une [notification séparée](#_Article_13_GDPR). Le système Mobileye 8 Connect pourrait ultérieurement collecter aussi des données télématiques ; celles-ci feront également l’objet d’une notification séparée, publiée en temps voulu.

### Les données DSR d’un véhicule à dispositif embarqué d’un parc automobile contiennent-elles des informations personnelles (« IP » désignant toute information relative à une personne physique identifiée ou identifiable) ?

A la différence des véhicules équipés d’origine, Mobileye reçoit les données DSR directement des véhicules à dispositif embarqué du parc automobile, mais ces DSR ne révèlent que le numéro de série des systèmes Mobileye 8 Connectspécifiques, installés sur les véhicules en question. A l’exception du cas stipulé ci-dessous, Mobileye ne dispose d’aucun moyen de faire correspondre ces systèmes aux véhicules sur lesquels ils ont été installés, car leurs numéros de série n’établissent strictement aucun lien avec une quelconque caractéristique (comme par ex. la plaque minéralogique) des véhicules qui en sont équipés. En tout cas, les numéros de série des systèmes Mobileye 8 Connectspécifiquessont définitivement et incessamment effacés dès réception des données DSR pertinentes.

Seule exception à la règle : si et seulement si le propriétaire d’un véhicule l’a explicitement autorisé. Dans ce cas, Mobileye ‘associera’ les systèmes à la *flotte* (parc automobile) à laquelle ces véhicules appartiennent, en remplaçant les numéros de série par un identifiant désignant le parc automobile concerné. De cette façon et dans ce cas, Mobileye saura que leurs données DSR ont été saisies par un véhicule appartenant au parc automobile ainsi désigné, *mais ne pourra pas identifier le véhicule spécifique*.

Le transit de toutes les données DSR envoyées à Mobileye sont protégées par des mesures techniques et organisationnelles.

Donc, le seul cas où des données DSR pourraient contenir des données IP est celui où elles sont ‘associées’ à une flotte particulière. Néanmoins, la présente notification est entièrement établie selon l’hypothèse que les DSR reçues par Mobileye des fabricants de véhicules à dispositif embarqué appartenant à un parc automobile, contiennent malgré tout, des infos IP.

### Que fait Mobileye des données de segment routier (DSR) ? (‘objectif de traitement’)

Mobileye consolide et organise le flux continu des DSR reçues depuis les véhicules pertinents, ce qui conduit à la formation d’une carte virtuelle de haute précision en temps réel, appelée « Roadbook™ » (Guide routier).

### Quel est le fondement légal permettant à Mobileye’s de collecter et d’utiliser les données DSR ? (‘légitimité du traitement’)

L’intérêt de Mobileye à collecter et à utiliser les données de segment routier (DSR) est légitime, celles-ci représentant un élément essentiel pour un écosystème de routier constitué de véhicules autonomes ou quasi-autonomes. La mise en service de véhicules autonomes est un objectif porteur d’un avantage social incontestable, celui de considérablement réduire les accidents de la route avec ce que cela implique de morts et de blessés.

### Transfert de données DSR hors Mobileye (‘types de destinataires des données IP’)

Mobileye est susceptible de partager des données DSR ‘brutes’ avec, par exemple, des cartographes.De telles données DSR, et *a fortiori*, un Roadbook (Guide routier) dérivé de DSR consolidées et organisées ne contiennent certes aucune information personnelle (IP). En cas de transfert de DSR vers d’autres pays, Mobileye s’appuie sur une combinaison de décisions d’adéquation de l’Union Européenne et de normes relatives à la protection des données.

### Délai de conservation des données RSD

Comme énoncé plus haut, l’utilisation principale des données DSR réside dans leur consolidation et leur organisation en un ‘Roadbook’ (Guide routier). Les données DSR brutes sont toutefois conservées tant qu’elles s’avèrent utiles.

### Droits des particuliers quant au respect de leurs informations personnelles (IP)

Les particuliers disposent de divers droits garantis par le RGPD (Règlement général sur la protection des données) quant aux données personnelles les concernant. Mobileye considèrera, au cas par cas, toute requête d’exercer ces droits.

### Droit des particuliers à déposer plainte

Tout particulier peut déposer une plainte auprès des autorités de surveillance locales. La liste de ces autorités de surveillance (telle qu’elle est vérifiée au jour de la publication de cet avis) est disponible [ici](http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm).