ANNEXE I

ACCORD SUR LE TRAITEMENT DES DONNÉES

Note relative à la traduction : le présent document constitue une traduction en langue française fournie à titre purement informatif. En cas de divergence, d'ambiguïté ou de contradiction entre la présente version française et la version anglaise du document, la version anglaise fait foi et prévaut à tous égards.

Préambule

Dans le cadre de l'exécution de la Solution et des Services IZIX, IZIX SRL et ses filiales peuvent être amenées à traiter des données personnelles de l'Utilisateur pour le compte et selon les instructions du Client. Le présent document définit les droits et obligations des Parties concernant le traitement des Données Personnelles, affirme leur engagement à traiter les Données Personnelles de manière sécurisée, délimite leurs rôles et responsabilités, et assure le respect de la Législation sur la Protection des Données applicable. La présente annexe s'applique spécifiquement au traitement des Données Personnelles par IZIX SRL.

Les Parties conviennent de ce qui suit :

1. Champ d'application

1.1 Dans le cadre et aux fins de l'exécution des Services IZIX en vertu du Contrat, les Données Personnelles sont traitées conformément aux dispositions du présent accord sur le traitement des données (le **«DPA»**).

1.2 Le Traitement des Données Personnelles est nécessaire à l'exécution des obligations d'IZIX en vertu du Contrat.

1.3 Le présent DPA énonce les conditions exclusives selon lesquelles les Données Personnelles sont traitées dans le cadre du Contrat.

2. Définitions

2.1 Les termes en majuscules non définis dans le présent article ont la signification qui leur est donnée dans la Législation sur la Protection des Données, le cas échéant, ou dans le Contrat.

2.2 Les termes en majuscules utilisés dans le Contrat ont la signification suivante :

2.2.1 **«Personne(s) de Contact»** désigne la ou les personnes désignées par une Partie et communiquées à l'autre Partie comme point de contact et représentant la Partie pour (une partie des) Services IZIX.

2.2.2 **«Responsable du Traitement»** désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement des Données Personnelles. Aux fins des Services IZIX, les Parties reconnaissent et conviennent que le Client est le Responsable du Traitement.

2.2.3 **«Sous-traitant»** désigne une personne physique ou morale, une autorité publique, un service ou tout autre organisme qui traite des Données Personnelles pour le compte du Responsable du Traitement. Dans le cadre du Contrat, les Parties reconnaissent et conviennent qu'IZIX est le Sous-traitant.

2.2.4 **«Législation sur la Protection des Données»** désigne le 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 (le **«Règlement Général sur la Protection des Données»** ou **«RGPD»**), ainsi que les codes de pratique, codes de conduite, lignes directrices réglementaires, clauses types et autres législations connexes résultant de ce règlement, tels que mis à jour de temps à autre.

2.2.5 **«Clauses Contractuelles Types»** désigne les clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers adoptées par la Commission européenne par la Décision d'exécution (UE) 2021/914 du 4 juin 2021 en vertu de l'article 46, paragraphe 2, point c), du RGPD, telles que modifiées, complétées ou remplacées de temps à autre. Le Module applicable est déterminé par la qualité en laquelle agit chaque partie au transfert.

3. Interprétation

3.1 Le présent DPA fait partie intégrante du Contrat. Sauf convention contraire, les dispositions du Contrat s'appliquent donc au présent DPA.

3.2 En cas de conflit entre une disposition du présent DPA et une disposition d'une autre partie du Contrat, le présent DPA prévaut.

4. Champ d'Application et Objet

4.1 Dans le cadre et aux fins de l'exécution des Services IZIX en vertu du Contrat, le Client charge IZIX de

traiter les Données Personnelles conformément aux dispositions du présent DPA.

4.2 Le Client peut être le Propriétaire, l'Occupant, ou les deux, au sens des Conditions Générales. Chaque Client agit en qualité de Responsable du Traitement pour les Données Personnelles dont il détermine les finalités et les moyens, et conclut le présent DPA en cette qualité.

4.3 Lorsque, pour un même Bâtiment, le Propriétaire et un ou plusieurs Occupants agissent tous deux en qualité de Responsable du Traitement, leurs champs respectifs sont les suivants :

4.3.1 le Propriétaire détermine le Traitement relatif à la configuration du Bâtiment et de ses Parkings, à l'attribution des droits de stationnement aux Occupants, et aux informations d'usage en résultant à ce niveau ;

4.3.2 chaque Occupant détermine le Traitement relatif aux Données Personnelles de ses propres Utilisateurs, y compris leur identification, leurs droits d'accès et leur usage individuel du stationnement.

4.4 IZIX agit sur les instructions documentées de chaque Responsable du Traitement dans les limites de son propre champ, et n'est pas responsable de la relation entre le Propriétaire et l'Occupant, ni d'une quelconque répartition des responsabilités convenue entre eux à laquelle IZIX n'est pas partie.

4.5 Lorsque IZIX reçoit d'un Propriétaire et d'un Occupant des instructions contradictoires, IZIX en informe les deux sans délai indu et agit sur les instructions du Responsable du Traitement dont relève le Traitement des Données Personnelles concernées conformément à l'article 4.3. Lorsque ce champ ne peut être raisonnablement déterminé, IZIX peut suspendre le Traitement litigieux jusqu'à ce que les Responsables du Traitement concernés l'aient informé par écrit de la position à adopter, sans encourir de responsabilité du fait de cette suspension.

4.6 Le présent DPA est conclu avec chaque Client, que ce soit par la signature d'un Bon de Commande ou par l'acceptation des documents constituant le Contrat conformément aux Conditions Générales. Lorsque le Propriétaire crée un Occupant sur le Système de Gestion de Parking, le Propriétaire garantit qu'il y est autorisé et informe cet Occupant que l'acceptation du Contrat, y compris du présent DPA, est requise. L'acceptation du présent DPA est enregistrée par IZIX conformément aux Conditions Générales, et cet enregistrement constitue une preuve entre les Parties.

5. Détails sur le Traitement des Données

5.1 Tout Traitement de Données Personnelles dans le cadre du Contrat est effectué conformément à la Législation sur la Protection des Données applicable et aux fins de l'exécution des Services IZIX en vertu du Contrat, y compris la fourniture de tout service aux Personnes Concernées elles-mêmes.

5.2 Pour l'exécution des Services IZIX, IZIX est un Sous-traitant agissant pour le compte du Client. En tant que Sous-traitant, IZIX n'agit que sur la base des instructions documentées du Client. Le Contrat, y compris le présent Accord sur le Traitement des Données, constitue l'intégralité des instructions du Client à IZIX en ce qui concerne le Traitement des Données Personnelles.

5.3 Toute instruction supplémentaire ou modifiée doit faire l'objet d'un accord écrit entre les Parties. Est réputé constituer une instruction donnée à IZIX de traiter des Données Personnelles :

5.3.1 le Traitement effectué conformément au Contrat ; ET

5.3.2 le Traitement initié par les Personnes Concernées ou tout Utilisateur dans le cadre de l'utilisation des Services IZIX.

5.4 Les Personnes Concernées sont tous les Utilisateurs de la Solution IZIX ou des Services IZIX, tels que décrits plus en détail dans le Contrat.

5.5 Les catégories de Données Personnelles traitées sont les suivantes :

5.5.1 Nom complet

5.5.2 Prénom

5.5.3 Nom de famille

5.5.4 Langue

5.5.5 Courriel

5.5.6 Téléphone

5.5.7 Plaque d'immatriculation

5.5.8 Utilisation du stationnement (qui/quand/pour quelle durée/quel parking) et réservations.

5.6 IZIX fournira au Client un accès aux Données Personnelles traitées dans le cadre du Contrat, afin de permettre au Client de consulter et de corriger ces Données Personnelles si nécessaire.

6. Droits des Personnes Concernées

6.1 En ce qui concerne la protection des droits des Personnes Concernées conformément à la Législation sur la Protection des Données applicable, le Client facilite l'exercice des droits des Personnes

Concernées et veille à ce qu'une information adéquate leur soit fournie sur le Traitement effectué en vertu des présentes, sous une forme concise, transparente, intelligible et facilement accessible, en des termes clairs et simples.

6.2 Si une Personne Concernée contacte directement IZIX pour exercer ses droits individuels, par exemple pour demander une copie, une rectification ou un effacement de ses données, ou pour restreindre ou s'opposer aux activités de Traitement, IZIX informe le Client de cette demande dans un délai de 2 jours ouvrables et lui en fournit tous les détails, ainsi qu'une copie des Données Personnelles qu'elle détient à l'égard de la Personne Concernée, le cas échéant. IZIX dirige rapidement cette Personne Concernée vers le Client. À l'appui de ce qui précède, IZIX peut fournir au demandeur les coordonnées de base du Client. Le Client s'engage à répondre à toute demande d'une Personne Concernée et à s'y conformer conformément aux dispositions de la Législation sur la Protection des Données applicable.

6.3 Dans la mesure du possible, IZIX coopère avec le Client et l'assiste, par des mesures techniques et organisationnelles appropriées, dans l'exécution de son obligation de répondre aux demandes des Personnes Concernées exerçant leurs droits.

7. Divulgation

7.1 IZIX ne divulguera aucune Donnée Personnelle à un Tiers, sauf dans les situations suivantes :

7.1.1 sur instruction du Client ;

7.1.2 comme stipulé dans le Contrat ;

7.1.3 dans la mesure requise pour le Traitement par des Sous-traitants Ultérieurs agréés conformément à l'Article 10 ; OU

7.1.4 lorsque la loi ou une autorité de régulation l'exige, auquel cas IZIX informera le Client de cette obligation légale avant de divulguer ces Données Personnelles, sauf si la loi applicable interdit la fourniture de cette information pour des motifs importants d'intérêt public.

7.2 IZIX déclare et garantit que les personnes agissant pour le compte d'IZIX et autorisées à traiter les Données Personnelles, ou à soutenir et gérer les systèmes traitant les Données Personnelles :

7.2.1 se sont engagées à préserver la sécurité et la confidentialité des Données Personnelles conformément aux dispositions du présent DPA ;

7.2.2 sont soumises à des processus d'authentification et de connexion de l'Utilisateur lorsqu'elles accèdent aux Données Personnelles ; ET

7.2.3 ont suivi une formation appropriée relative aux obligations découlant de la Législation sur la Protection des Données.

7.3 IZIX informe les personnes agissant pour son compte des exigences applicables et veille à leur respect au moyen d'obligations de confidentialité contractuelles ou légales.

8. Suppression et Restitution des Données Personnelles

8.1 Au plus tard dans les 30 jours suivant la résiliation du Contrat, IZIX devra, à la discrétion du Client, anonymiser ou détruire toute Donnée Personnelle qu'elle conserve, d'une manière sécurisée garantissant que toute Donnée Personnelle est anonymisée ou supprimée et irrécupérable. Les Données Personnelles utilisées pour vérifier le bon Traitement des données conformément à la mission, ou qui doivent être conservées pour se conformer aux exigences légales et réglementaires de conservation applicables, peuvent être conservées par IZIX au-delà de la résiliation ou de l'expiration du Contrat, dans la seule mesure requise par ces lois ou réglementations.

8.2 Sur demande écrite du Client soumise au plus tard 14 jours calendaires avant la résiliation ou l'expiration du Contrat, IZIX fournira au Client une copie lisible et utilisable des Données Personnelles et/ou des systèmes contenant des Données Personnelles avant leur anonymisation ou destruction.

9. Lieu de Traitement

9.1 IZIX stocke les Données Personnelles au repos sur le territoire de l'Espace Économique Européen (EEE).

9.2 Tout Traitement de Données Personnelles par du personnel ou des sous-traitants d'IZIX non situés dans l'EEE ne peut être effectué que conformément aux dispositions du présent DPA ou après approbation écrite préalable du Client et mise en œuvre de l'un des mécanismes de transfert de données alors légalement reconnus, tel qu'un accord de traitement de données supplémentaire régi par les Clauses Contractuelles Types.

9.3 Lorsque IZIX confie le Traitement de Données Personnelles à un Sous-traitant Ultérieur établi hors de l'EEE dans un pays non couvert par une décision d'adéquation de la Commission européenne, ce transfert est régi par le Module Trois (sous-traitant à sous-traitant) des Clauses Contractuelles Types conclues entre IZIX et le Sous-traitant Ultérieur concerné, complétées si nécessaire par les mesures techniques, organisationnelles et contractuelles

supplémentaires identifiées au moyen d'une analyse d'impact relative au transfert.

10. Sous-traitance Ultérieure

10.1 Le Client reconnaît et accepte expressément qu'IZIX puisse recourir à des Sous-traitants Ultérieurs pour la fourniture des Services IZIX tels que décrits dans le Contrat.

10.2 Tout Sous-traitant Ultérieur qui fournit des services à IZIX et traite des Données Personnelles pour son compte n'est autorisé à traiter ces Données Personnelles que pour fournir les services qui lui ont été confiés par IZIX, et il lui est interdit de traiter ces Données Personnelles à toute autre fin. IZIX demeure pleinement responsable du respect, par un tel Sous-traitant Ultérieur, des obligations d'IZIX au titre du Contrat, y compris du présent DPA.

10.3 Préalablement à confier des services à un Sous-traitant Ultérieur, IZIX effectuera toute diligence appropriée sur ce Sous-traitant Ultérieur afin d'évaluer sa capacité à assurer le niveau de protection des Données Personnelles requis par le présent DPA, et fournira la preuve de cette diligence au Client lorsque celui-ci ou une autorité de régulation le demande.

10.4 IZIX conclura avec tout Sous-traitant Ultérieur des accords écrits contenant des obligations au moins aussi protectrices que celles du présent DPA, s'agissant de la protection des Données Personnelles dans la mesure applicable à la nature des Services IZIX fournis par ce Sous-traitant Ultérieur, y compris les obligations imposées par les Clauses Contractuelles Types, le cas échéant.

10.5 Sur demande écrite du Client, IZIX mettra à sa disposition la liste actuelle des Sous-traitants Ultérieurs pour la fourniture des Services IZIX.

10.6 Si le Client s'oppose au recours à un nouveau Sous-traitant Ultérieur qui traiterait ses Données Personnelles, il doit en informer IZIX par écrit dans un délai de 30 jours calendaires après avoir été informé des activités de traitement de ce Sous-traitant Ultérieur. Dans ce cas, IZIX s'efforcera raisonnablement de modifier les Services concernés ou de recommander au Client une modification commercialement raisonnable de son utilisation des Services concernés afin d'éviter le Traitement des Données Personnelles par le Sous-traitant Ultérieur concerné. Si IZIX n'est pas en mesure de mettre à disposition ou de proposer une telle modification dans un délai de 60 jours calendaires, le Client peut résilier la partie du Contrat relative aux Services qui ne peuvent être fournis par IZIX sans recourir au Sous-traitant Ultérieur concerné. À cette fin, le Client doit notifier la résiliation par écrit en indiquant les motifs raisonnables de son refus.

11. Mesures Techniques et Organisationnelles

11.1 IZIX a mis en œuvre et maintiendra des mesures techniques et organisationnelles appropriées destinées à protéger les Données Personnelles ou les systèmes traitant les Données Personnelles contre tout accès, divulgation, altération, perte ou destruction accidentels, non autorisés ou illicites. Ces mesures tiennent compte de, et sont adaptées à, l'état de l'art, la nature, la portée, le contexte et les finalités du Traitement, ainsi qu'au risque de préjudice pouvant résulter d'un Traitement non autorisé ou illicite ou d'une perte, destruction ou altération accidentelle des Données Personnelles. Ces mesures comprennent toujours les mesures suivantes :

11.1.1 empêcher toute personne non autorisée d'accéder aux systèmes traitant des Données Personnelles (contrôle d'accès physique) ;

11.1.2 empêcher toute utilisation non autorisée des systèmes traitant des Données Personnelles (contrôle d'accès logique) ;

11.1.3 veiller à ce que les personnes habilitées à utiliser un système traitant des Données Personnelles n'accèdent qu'aux Données Personnelles auxquelles elles ont droit d'accéder conformément à leurs droits d'accès, et à ce que, au cours du Traitement, les Données Personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation (contrôle d'accès aux données) ;

11.1.4 veiller à ce que les Données Personnelles ne puissent être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transmission électronique, de leur transport ou de leur stockage sur des supports, et à ce que les destinataires de tout transfert de Données Personnelles au moyen d'installations de transmission de données puissent être établis et vérifiés (contrôle du transfert de données) ;

11.1.5 garantir la mise en place d'une piste d'audit permettant de documenter si et par qui des Données Personnelles ont été introduites, modifiées ou supprimées dans les systèmes traitant des Données Personnelles (contrôle des entrées) ;

11.1.6 veiller à ce que les Données Personnelles traitées le soient uniquement conformément aux instructions (contrôle des instructions) ;

11.1.7 veiller à ce que les Données Personnelles soient protégées contre toute destruction ou perte accidentelle (contrôle de la disponibilité) ;

11.1.8 veiller à ce que les Données Personnelles collectées à des fins différentes puissent être traitées séparément (contrôle de la séparation).

11.2 IZIX adaptera systématiquement les mesures techniques et organisationnelles à l'évolution de la réglementation, de la technologie et d'autres aspects, et les complétera par les mesures techniques et organisationnelles applicables des Sous-traitants Ultérieurs, le cas échéant. En tout état de cause, les mesures techniques et organisationnelles mises en œuvre assureront un niveau de sécurité adapté aux risques présentés par le Traitement et à la nature des Données Personnelles à protéger, compte tenu également de l'état de la technique et du coût de leur mise en œuvre.

11.3 Sur demande écrite du Client, IZIX lui fournira, dans un délai de 14 jours calendaires à compter de la réception de la demande par IZIX, une description des mesures techniques et organisationnelles de protection mises en œuvre.

12. Violations de Données Personnelles

12.1 En cas de Violation de Données Personnelles (probable ou avérée), et quelle qu'en soit la cause, IZIX notifiera le Client sans délai indu et au plus tard dans les 48 heures après avoir pris connaissance (de la probabilité ou de la survenance) d'une telle Violation de Données Personnelles, en lui fournissant des informations suffisantes et dans un délai permettant au Client de satisfaire à toute obligation de signalement d'une Violation de Données Personnelles au titre de la Législation sur la Protection des Données. Cette notification précisera au minimum :

12.1.1 la nature de la Violation de Données Personnelles ;

12.1.2 la nature ou le type de Données Personnelles concernées par la Violation de Données Personnelles, ainsi que les catégories et le nombre de Personnes Concernées ;

12.1.3 les conséquences probables de la Violation de Données Personnelles ;

12.1.4 selon le cas, les mesures correctives prises ou envisagées pour atténuer les effets et minimiser tout dommage résultant de la Violation de Données Personnelles ;

12.1.5 l'identité et les coordonnées du Délégué à la Protection des Données ou d'une autre Personne de Contact auprès de laquelle des informations complémentaires peuvent être obtenues.

12.2 IZIX poursuivra sans délai indu son enquête sur la Violation de Données Personnelles, tiendra le Client informé de l'avancement de l'enquête, et prendra des mesures raisonnables pour en minimiser davantage l'impact. Les deux Parties conviennent de coopérer pleinement à cette enquête et de s'entraider dans le respect de toute exigence et procédure de notification.

12.3 L'obligation d'une Partie de signaler ou de répondre à une Violation de Données Personnelles ne constitue pas, et ne saurait être interprétée comme, une reconnaissance par cette Partie d'une faute ou d'une responsabilité quelconque relative à cette Violation de Données Personnelles.

13. Audit

13.1 IZIX met à la disposition du Client toute information raisonnable, dans le cadre du Contrat, pour démontrer le respect de ses obligations au titre du présent DPA ou de la Législation sur la Protection des Données applicable. IZIX permet notamment les audits, y compris les inspections, menés par le Client ou un autre auditeur mandaté par le Client, conformément au présent DPA, et y contribue.

13.2 Si les informations et rapports fournis par IZIX au titre du présent article sont insuffisants pour permettre au Client de démontrer que les obligations découlant de la Législation sur la Protection des Données sont respectées, les Parties se réuniront pour convenir des modalités opérationnelles, de sécurité et financières d'une inspection technique sur site. En tout état de cause, les conditions de cette inspection ne devront pas porter atteinte à la sécurité des autres clients d'IZIX.

13.3 Les droits d'information et d'audit du Client n'existent que dans la mesure où le Contrat ne lui confère pas par ailleurs des droits d'information et d'audit répondant aux exigences de la Législation sur la Protection des Données applicable. Le Client, ou la personne qu'il mandate pour effectuer un audit, doit informer IZIX ou le partenaire concerné d'IZIX de tout audit ou inspection à réaliser, et fait tout son possible (et veille à ce que chaque auditeur mandaté fasse tout son possible) pour éviter de causer (ou, à défaut, minimiser) tout dommage, blessure ou perturbation aux locaux, équipements, personnel et opérations d'IZIX pendant que le personnel d'IZIX se trouve dans ces locaux au cours d'un tel audit ou inspection.

13.4 IZIX n'est pas tenue de donner accès à ses locaux aux fins d'un tel audit ou d'une telle inspection :

13.4.1 à une personne ne disposant pas d'une preuve raisonnable de son identité et de ses droits ;

13.4.2 en dehors des heures normales d'ouverture de ses locaux, sauf si l'audit ou l'inspection doit être réalisé en urgence et que le Client, ou la personne qu'il mandate, a informé IZIX ou le partenaire concerné d'IZIX que l'audit doit être réalisé avant les heures d'ouverture.

13.5 Si plus d'un audit ou d'une inspection a lieu au cours d'une année calendaire, des frais supplémentaires peuvent être facturés au Client, à l'exception des audits ou inspections supplémentaires lorsque :

13.5.1 le Client, ou la personne liée au Client réalisant l'audit, l'estime raisonnablement nécessaire en raison de préoccupations réelles quant au respect du DPA par IZIX, ou par une personne liée à IZIX ; ou

13.5.2 le Client est tenu par une loi sur la protection des données, une autorité de protection des données ou une autorité de régulation similaire chargée de l'application des lois sur la protection des données, de réaliser cet audit.

13.6 En outre, IZIX accorde au Client un accès raisonnable pour vérifier et/ou auditer la conformité d'IZIX au DPA, aux conditions suivantes :

13.6.1 toute vérification ou inspection est limitée aux activités de traitement et aux installations directement impliquées dans le Traitement des Données Personnelles ;

13.6.2 le Client donne à IZIX un préavis écrit raisonnable d'au moins 30 jours avant tout audit ou inspection (sauf délai plus court exigé par la loi, une autorité de régulation, ou convenu autrement par les Parties) ;

13.6.3 le Client réalise l'audit ou l'inspection pendant les heures normales d'ouverture et sans créer d'interruption d'activité pour IZIX, sauf accord contraire avec IZIX ;

13.6.4 IZIX n'est pas tenue de divulguer ou de donner accès à des informations relatives à ses propres activités commerciales ou à des tiers envers lesquels elle a une obligation de confidentialité ;

13.6.5 l'audit ou l'inspection est mené conformément aux politiques et procédures d'IZIX applicables sur site, y compris, sans s'y limiter, celles relatives à l'accès aux locaux, à l'équipement, à la sécurité, à la santé, à la sûreté et aux données ;

13.6.6 lorsque l'audit ou l'inspection est réalisé par un tiers pour le compte du Client, ce tiers est soumis à des obligations équivalentes à celles du DPA et ne peut être un concurrent d'IZIX ;

13.7 l'inspection sur site susmentionnée, ainsi que la communication de certificats et de rapports d'inspection, peuvent donner lieu à une facturation supplémentaire raisonnable.

13.8 Nonobstant ce qui précède, le Client est autorisé à répondre aux demandes de l'autorité de contrôle compétente, à condition que toute divulgation d'informations soit strictement limitée à ce qui est demandé par cette autorité. Dans ce cas, et sauf interdiction du droit applicable, le Client doit d'abord consulter IZIX.

13.9 Dans le cas où (1) l'audit nécessite la coopération d'un fournisseur d'hébergement de données ou d'un autre prestataire de services informatiques, agissant en tant que Sous-traitant Ultérieur d'IZIX, et (2) ce Sous-traitant Ultérieur est une société majeure dont les accords de traitement de données ne sont pas soumis à négociation avec le Responsable du Traitement (par exemple : AWS, Microsoft Azure, OVH, etc.), le Client accepte expressément que, dans la mesure où ce Sous-traitant Ultérieur et ses systèmes sont concernés, les dispositions d'audit figurant dans l'accord de traitement des données de ce Sous-traitant Ultérieur soient contraignantes et, par conséquent, opposables au Client. Cet accord de traitement des données peut être obtenu directement auprès du Sous-traitant Ultérieur ou sur demande écrite du Client.

14. Responsabilités du Client

14.1 Le Client se conforme à toutes les lois et réglementations applicables, y compris la Législation sur la Protection des Données.

14.2 Le Client demeure responsable de la licéité du Traitement des Données Personnelles, y compris, le cas échéant, de l'obtention du consentement des Personnes Concernées au Traitement de leurs Données Personnelles.

14.3 Le Client prend des mesures raisonnables pour tenir à jour les Données Personnelles afin qu'elles ne soient pas inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées.

14.4 S'agissant des composants que le Client fournit ou contrôle, y compris, sans s'y limiter, les postes de travail se connectant aux Services, les mécanismes de transfert de données utilisés et les identifiants délivrés au personnel du Client, le Client met en œuvre et maintient les mesures techniques et

organisationnelles requises pour la protection des Données Personnelles.

15. Notifications

15.1 Sauf interdiction légale, IZIX informera le Client dès que raisonnablement possible, et au plus tard dans les 2 jours ouvrables suivant sa prise de connaissance des circonstances pertinentes, si elle-même ou l'un de ses Sous-traitants Ultérieurs :

15.1.1 reçoit une demande de renseignements, une citation à comparaître ou une demande d'inspection ou d'audit émanant d'une autorité publique compétente concernant le Traitement ;

15.1.2 envisage de divulguer des Données Personnelles à une autorité publique compétente en dehors du cadre des Services prévus par le Contrat. À la demande du Client, IZIX fournira une copie des documents remis à l'autorité compétente ;

15.1.3 reçoit une instruction qui enfreint la Législation sur la Protection des Données ou les obligations du présent DPA ;

15.2 IZIX coopérera, à la demande du Client, pour permettre à ce dernier de se conformer à toute évaluation, enquête, notification ou investigation au titre de la Législation sur la Protection des Données, ce qui inclut la fourniture :

15.2.1 de toutes les données demandées par le Client (qui ne sont pas autrement à sa disposition) dans le délai raisonnable précisé par le Client dans chaque cas, y compris le détail complet et les copies de la plainte, de la communication ou de la demande, ainsi que toute Donnée Personnelle qu'elle détient à l'égard de la ou des Personne(s) Concernée(s) ; ET

15.2.2 le cas échéant, de l'assistance raisonnablement demandée par le Client pour lui permettre de se conformer aux articles 32 à 36 du RGPD et à la demande concernée dans les délais légaux prévus par la Législation sur la Protection des Données.

15.3 Toute notification au titre du présent DPA, y compris une notification de Violation de Données Personnelles, sera adressée à une ou plusieurs Personnes de Contact du Client par e-mail, éventuellement complété par tout autre moyen choisi par IZIX. Sur demande du Client, IZIX lui fournira un aperçu des coordonnées de ses Personnes de Contact enregistrées. Il incombe exclusivement au Client de signaler en temps utile tout changement de coordonnées et de veiller à ce que les coordonnées de ses Personnes de Contact demeurent exactes.

16. Durée et Résiliation

16.1 Le présent DPA entre en vigueur en même temps que le Contrat et demeure en vigueur jusqu'à ce que le Traitement des Données Personnelles par IZIX ne soit plus nécessaire dans le cadre ou en vertu du Contrat.

DATE DE LA DERNIÈRE MISE À JOUR : 28 juillet 2026

ANNEXES À L'ANNEXE I

ACCORD SUR LE TRAITEMENT DES DONNÉES

Les annexes suivantes font partie intégrante de l'Annexe I – Accord sur le Traitement des Données aux Conditions Générales d'IZIX.

ANNEXE 1 – SERVICES FOURNIS ET DÉTAILS DES DONNÉES PERSONNELLES TRAITÉES

ACTIVITÉS DE TRAITEMENT	NATURE DES OPÉRATIONS EFFECTUÉES ET FINALITÉ DU TRAITEMENT DES DONNÉES	PERSONNE CONCERNÉE	TYPE DE DONNÉES	DURÉE DE CONSERVATION DES DONNÉES
Exécution des Services IZIX (gestion de l'accès au stationnement via la Solution numérique IZIX)	Création et gestion des comptes du Client	Utilisateurs	- Coordonnées (nom complet, prénom, nom de famille, e-mail, numéro de téléphone) ; - Langues ; - Plaque d'immatriculation ; - Utilisation du stationnement et réservations.	La politique de conservation des données relève de la responsabilité du Responsable du Traitement.
	Gestion de l'accès au stationnement		- Coordonnées (nom complet, prénom, nom de famille) ; - Plaque d'immatriculation ; - Utilisation du stationnement et réservations.	
	Gestion des paiements pour les Services IZIX		- Coordonnées (nom complet, prénom, nom de famille, e-mail) ; - Détails et titulaire de la carte de crédit ; - Adresse ; - Pays d'origine.	

Nature du traitement : opérations effectuées sur les données (accès, gestion, stockage, etc.). Finalité : l'objectif pour lequel les données sont collectées, enregistrées, traitées, transmises, stockées, etc.

Personne concernée : les personnes dont les données personnelles sont traitées dans le cadre de la sous-traitance.

Type de données : toute donnée personnelle de quelque nature que ce soit traitée dans le cadre de la sous-traitance et des services fournis par le sous-traitant au Responsable du Traitement (pouvant inclure notamment des données d'identification, des données financières et des données sensibles, en particulier des données de santé).

Durée de conservation des données : la durée du Contrat, ou une durée plus courte selon la nature des services fournis dans le cadre du Contrat.

ANNEXE 2 – SOUS-TRAITANTS ULTÉRIEURS AUTORISÉS

Dès la signature du DPA, IZIX est autorisée à recourir aux Sous-traitants Ultérieurs suivants :

1. Sous-traitants Ultérieurs Généraux d'IZIX

NOM	LOCALISATION	ACTIVITÉ DE TRAITEMENT EXTERNALISÉE
AWS (ISO27001)	EEE (Irlande et Allemagne)	Services d'hébergement et de centre de données
Sentry	EEE	Services de journalisation et de surveillance

Mailjet	EEE	Services d'e-mails transactionnels
Pusher	EEE	Services de notification en temps réel
Papertrail	EEE	Services de journalisation et de surveillance

2. Sous-traitants Ultérieurs liés à des services spécifiques d'IZIX

NOM	LOCALISATION	ACTIVITÉ DE TRAITEMENT EXTERNALISÉE
Stripe Payments Europe, Limited (SPEL)	EEE	Prestataire de services de paiement sécurisé pour la fonctionnalité de Crédit Prépayé
Aria Group (ISO27001)	Maroc	Assistance téléphonique pour le service Parking Desk et fourniture d'une assistance complémentaire liée à la prestation des services IZIX

ANNEXE 3 – MESURES TECHNIQUES ET ORGANISATIONNELLES

1. Sécurité des centres de données et des réseaux

Sécurité physique

1.1. Installations : les serveurs IZIX sont hébergés sur AWS, dans des installations conformes SOC 2 Type II et ISO 27001, situées à l'intérieur des frontières de l'Union européenne. En outre, les installations des centres de données sont alimentées par une alimentation redondante, chacune équipée d'un onduleur (UPS) et de générateurs de secours. Par ailleurs, les fournisseurs d'hébergement n'ont pas accès aux données des clients.

1.2. Sécurité sur site : nos installations de centres de données sont sécurisées par un périmètre de zones de sécurité à plusieurs niveaux, une équipe de sécurité présente 24h/24 et 7j/7, et une vidéosurveillance CCTV. Elles sont en outre sécurisées par une identification multifactorielle avec contrôle d'accès biométrique, verrous physiques et alarmes en cas d'atteinte à la sécurité. Nos locaux de bureaux sont sécurisés par des systèmes de contrôle d'accès nominatifs et une vidéosurveillance. Par ailleurs, les points d'accès Wifi sont protégés par des mots de passe robustes conservés dans des gestionnaires de mots de passe. Un Wifi invité est fourni afin d'éviter que des tiers ne se connectent au Wifi principal. Le verrouillage automatique et la protection par mot de passe des ordinateurs sont appliqués à l'échelle de l'entreprise.

1.3. Surveillance : un système de surveillance automatique est en place pour vérifier en permanence l'état des services, envoyant des alertes au personnel approprié d'IZIX si nécessaire. La sécurité physique, l'alimentation électrique et la connectivité internet sont surveillées par les fournisseurs d'installations.

Sécurité des réseaux

1.4. Protection : notre réseau est protégé par des pare-feux redondants, un transport HTTPS sécurisé sur les réseaux publics, des audits réguliers et des systèmes de détection d'intrusion (IDS) qui surveillent et/ou bloquent le trafic malveillant et les attaques réseau.

1.5. Architecture : l'architecture de sécurité de notre réseau comprend plusieurs zones de sécurité. Les systèmes les plus sensibles, tels que les serveurs de base de données, sont protégés dans nos zones les plus fiables, non accessibles depuis l'internet public. Les données transférées entre serveurs IZIX transitent par un réseau privé.

1.6. Tests d'intrusion par des tiers : outre notre vaste programme interne d'analyse et de test, des tests d'intrusion sont réalisés chaque année.

1.7. Accès logique : l'accès au réseau de production IZIX est restreint selon le principe du besoin d'en connaître explicite, en appliquant le principe du moindre privilège. Il fait l'objet d'audits et d'une surveillance fréquents, et est contrôlé par notre équipe de direction. Les employés accédant aux serveurs de production IZIX sont tenus d'utiliser plusieurs facteurs d'authentification lorsque cela est pris en charge.

1.8. Réponse aux incidents de sécurité : en cas d'alerte système, les événements sont escaladés vers nos équipes disponibles 24h/24 et 7j/7. Les employés sont formés aux processus de réponse aux incidents de sécurité, y compris les canaux de communication et les procédures d'escalade.

Chiffrement

1.9. Chiffrement en transit : les communications entre vous et les serveurs IZIX sont chiffrées selon les meilleures pratiques du secteur : HTTPS et Transport Layer Security 1.2 (ou 1.3) (TLS) avec un chiffrement AES-256 standard sur les réseaux publics. AES-256 est un algorithme de chiffrement à 256 bits utilisé pour la transmission de données dans le cadre du TLS. Les clés cryptographiques sont protégées par des certificats reposant sur l'algorithme de signature SHA256.

1.10. Chiffrement au repos : les disques durs de tous les serveurs sont chiffrés grâce à un système de fichiers chiffré qui chiffre l'ensemble de vos données et métadonnées au repos à l'aide d'un algorithme de chiffrement AES-256 standard du secteur. Les clés cryptographiques sont protégées par des certificats reposant sur l'algorithme de signature SHA256.

Disponibilité et continuité

1.11. Redondance : IZIX met en œuvre un regroupement de services et des redondances réseau afin d'éliminer les points de défaillance uniques. Notre régime de sauvegarde strict garantit que les données des clients sont activement répliquées dans des centres de données géographiquement distincts.

1.12. Reprise après sinistre : notre programme de reprise après sinistre (DR) garantit que nos services demeurent disponibles ou sont facilement récupérables en cas de sinistre. Cela est réalisé en construisant un environnement technique robuste et en établissant des plans de reprise après sinistre continuellement mis à jour et testés.

2. Sécurité applicative

Développement sécurisé

2.1. Formation à la sécurité : les ingénieurs suivent une formation au code sécurisé couvrant les 10 principales failles de sécurité de l'OWASP, les vecteurs d'attaque courants et les contrôles de sécurité d'IZIX.

2.2. Assurance qualité et couverture du code : nos ingénieurs QA dédiés testent tous les développements logiciels au moyen de tests automatisés et manuels avant la mise en production. Nous visons une couverture de code très élevée sur l'ensemble des applications IZIX.

2.3. Environnements séparés : les environnements de test et de préproduction sont séparés physiquement et logiquement de l'environnement de production.

2.4. Processus de déploiement CI/CD : IZIX utilise le processus de déploiement CI/CD (intégration continue, déploiement continu). Celui-ci joue un rôle essentiel dans le maintien de normes de sécurité élevées grâce à la détection

précoce des anomalies, aux tests automatisés, au contrôle de la qualité du code, aux contrôles automatisés de sécurité et de conformité, et aux mécanismes de retour arrière (rollback). Cela permet à la fois de garantir la qualité du code déployé et d'assurer une réponse rapide en cas de problème.

2.5. Correctifs : les correctifs et mises à jour des systèmes sont effectués selon les besoins, dans le respect des contraintes et procédures normales de déploiement.

Vulnérabilités applicatives

2.6. Analyse statique du code : les dépôts de code source sont analysés en continu pour détecter les problèmes de sécurité grâce à notre outil d'analyse statique intégré. Toute modification de code est analysée par ces outils avant sa mise en production, dans le cadre de la procédure standard de notre processus de publication CI/CD.

2.7. Tests d'intrusion de sécurité : la sécurité applicative fait également partie des tests d'intrusion annuels réalisés par des experts tiers.

3. Fonctionnalités de sécurité du produit

Sécurité de l'authentification

3.1. Options d'authentification : IZIX propose des options d'authentification comprenant nom d'utilisateur/mot de passe, SSO via OAuth et SAML 2.0. L'objectif est de rendre IZIX compatible avec la plupart des portails SSO. L'API et les systèmes distants peuvent également se connecter via OAuth 2.0. Les données de mot de passe sont toujours hachées et chiffrées. La méthode d'authentification est définie par le Client pour son propre environnement IZIX.

3.2. Gestion sécurisée des identifiants : pour le stockage sécurisé des identifiants, IZIX applique les meilleures pratiques : stockage des identifiants dans un système de gestion des mots de passe. Les composants d'infrastructure et les systèmes cloud sont protégés par une politique stricte de mots de passe et des jetons de courte durée.

3.3. Sécurité et authentification de l'API : l'API IZIX est exclusivement SSL. L'utilisateur ou le tiers doit être un utilisateur vérifié pour effectuer des requêtes API. L'accès à l'API et l'authentification sont possibles via les protocoles OAuth 2.0. En outre, l'utilisateur ou le tiers doit disposer des autorisations et des périmètres (scopes) API appropriés pour accéder aux données des clients.

Fonctionnalités de sécurité supplémentaires du produit

3.4. Droits d'accès et rôles : l'accès aux données au sein d'IZIX est régi par des droits d'accès et peut être configuré pour définir des privilèges d'accès granulaires. IZIX dispose de différents niveaux d'autorisation pour les utilisateurs (par exemple, Admin, Réception, Sécurité, Assistants, etc.).

3.5. Sécurité des transmissions : toutes les communications avec les serveurs IZIX sont chiffrées selon les normes du secteur HTTPS et TLS 1.2 et 1.3 sur les réseaux publics. Cela garantit que l'ensemble du trafic entre vous et IZIX demeure sécurisé pendant la transmission.

3.6. Séparation des données : la segmentation logique des données des clients est appliquée au niveau du code, empêchant efficacement l'accès aux données d'un client par un autre.

3.7. Conservation des données : vous pouvez supprimer automatiquement les profils après une période de conservation donnée, ce qui facilite la conformité aux réglementations en matière de protection de la vie privée telles que le RGPD.

3.8. Piste d'audit : des pistes d'audit comprenant l'heure de la modification et l'utilisateur responsable de celle-ci sont en place pour les objets critiques.

3.9. Sous-traitants Ultérieurs : IZIX sélectionne avec soin ses sous-traitants ultérieurs de données tiers et les évalue régulièrement. Tous ces sous-traitants ultérieurs sont contractuellement tenus par IZIX de préserver la confidentialité des données des clients.

3.10. Prévention des injections JS : afin de prévenir les injections JavaScript, nous avons mis en œuvre des mesures robustes au niveau du code. Notre approche comprend une validation rigoureuse des entrées, des politiques de sécurité du contenu qui restreignent et contrôlent efficacement les ressources que le navigateur est autorisé à charger, ainsi que la formation du personnel d'ingénierie aux pratiques de codage sécurisé.

4. Certifications de conformité, adhésions et évaluations externes

4.1. RGPD : IZIX est en totale conformité avec le RGPD. Veuillez vous référer à la Politique de Confidentialité et à l'Accord sur le Traitement des Données.

4.2. SecurityScorecard : SecurityScorecard est une société de sécurité de l'information qui collecte, attribue et évalue l'état général de la cybersécurité des entreprises par l'identification des vulnérabilités exposées sur les actifs numériques des entreprises découverts sur l'internet public. Le score d'IZIX est A.

4.3. Niveau A : nos points de terminaison d'API et d'application sont exclusivement TLS/SSL. Cela signifie que les communications entre vous et les serveurs IZIX sont chiffrées selon les meilleures pratiques du secteur : HTTPS et Transport Layer Security (TLS) sur les réseaux publics.

5. Méthodologies de sécurité supplémentaires

5.1. Politiques : IZIX a élaboré un ensemble complet de politiques de sécurité couvrant un large éventail de sujets. Ces politiques sont partagées et mises à la disposition de tous les employés et contractants ayant accès aux actifs informationnels d'IZIX.

5.2. Vérification des antécédents : IZIX effectue des vérifications d'antécédents pour tous les nouveaux employés conformément aux lois locales. Ces vérifications incluent des contrôles d'antécédents judiciaires. Tous les employés nouvellement embauchés font l'objet d'un contrôle dans le cadre du processus de recrutement et sont tenus de signer des accords de non-divulgation et de confidentialité.

5.3. Intégration et départ des employés (onboarding et offboarding) : les politiques d'intégration et de départ d'IZIX

garantissent que les droits d'accès ne sont accordés qu'une fois la formation appropriée suivie et les critères de sécurité nécessaires satisfaits. De même, tout droit d'accès sensible est supprimé lorsqu'un employé quitte l'entreprise ou le projet, ou immédiatement en cas de faute grave.