APPENDIX I: DATA PROCESSING AGREEMENT

Index

1. PREAMBLE

1.1 In connection with and for the purpose of the performance of the IZIX Services under the Agreement, Personal Data shall be processed in accordance with the provisions of the present data processing agreement (the "**DPA**").

1.2 Processing of Personal Data is necessary for the performance of IZIX obligations under the Agreement.

1.3 This DPA sets forth the exclusive terms and conditions pursuant to which Personal Data shall be processed in the framework of the Agreement.

2. DEFINITIONS

2.1 Capitalized words not defined in this article shall have the meaning set forth in Data Protection Legislation where relevant, or in the Agreement.

2.2 Capitalized words used in the Agreement shall exclusively have the following meaning:

2.2.1 "**Contact Person(s)**" means the individual(s) assigned by a Party and communicated to the other Party as point of contact and representing the Party for (a part of) IZIX Services.

2.2.2 "**Data Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data. For the purposes of IZIX Services, the Parties acknowledge and agree that the Customer is the Data Controller.

2.2.3 "**Data Processor**" means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Data Controller. In the context of the Agreement, the Parties acknowledge and agree that IZIX is the Data Processor.

2.2.4 "**Data Protection Legislation**" means EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**General Data Protection Regulation**" or "**GDPR**") together with the codes of practice, codes of conduct, regulatory guidance and standard clauses and other related legislation resulting from such Regulation, as updated from time to time.

2.2.5 "**Standard Contractual Clauses**" means the standard contractual clauses of which the European Commission on the basis of Article 26 (4) of Directive 95/46/EC decided that these offer sufficient safeguards for the transfers of Personal Data to a third country, or the data protection clauses adopted by the European Commission or by a supervisory authority and approved by the European Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR. In the event of any such data protection clauses adopted in accordance with the GDPR, such clauses shall prevail over any standard contractual clauses adopted on the basis of Directive 95/46/EC to the extent that they intend to cover the same kind of data transfer relationship.

3. INTERPRETATION

3.1 This DPA forms an integral part of the Agreement. Unless otherwise agreed, the provisions of the Agreement therefore apply to this DPA.

3.2 In case of conflict between any provision in this DPA and any provision of another part of the Agreement, this DPA shall prevail.

4. SCOPE AND PURPOSE

4.1 In connection with and for the purpose of the performance of IZIX Services under the Agreement, the Customer commissions IZIX to process Personal Data in accordance with the provisions of this DPA.

5. DETAILS ABOUT DATA PROCESSING

5.1 Any Processing of Personal Data under the Agreement shall be performed in accordance with the applicable Data Protection Legislation and for the purpose of the performance of IZIX Services under the Agreement, including providing any services to the Data Subjects themselves.

5.2 For the performance of IZIX Services, IZIX is a Data Processor acting on behalf of the Customer. As a Data Processor, IZIX shall only act upon Customer's documented instructions. The Agreement, including this Data Processing Agreement, form the Customer's complete instructions to IZIX with regard to the Processing of Personal Data.

5.3 Any additional or modified instructions must be jointly agreed upon by the Parties in writing. The following is deemed an instruction to IZIX to Process Personal Data:

5.3.1 Processing in accordance with the Agreement; AND

5.3.2 Processing initiated by the Data Subjects or any Users in their use of IZIX Services.

5.4 Data Subjects are all Users of the IZIX Solution or of IZIX Services, as further described in the Agreement.

5.5 The relevant categories of Personal Data processed are the following:

5.5.1 Full Name
5.5.2 First name
5.5.3 Last name
5.5.4 Language
5.5.5 Email
5.5.6 Phone
5.5.7 Licence plate
5.5.8 Usage of parking (who/when/for how long/which parking) and bookings.

5.6 IZIX shall provide the Customer with access to Personal Data Processed under the Agreement, in order to allow the Customer to consult and correct such Personal Data if necessary.

6. RIGHTS OF DATA SUBJECTS

6.1 With regard to the protection of Data Subjects' rights pursuant to the applicable Data Protection Legislation, the Customer shall facilitate the exercise of Data Subject rights and shall ensure that adequate information is provided to Data Subjects about the Processing hereunder in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

6.2 5Should a Data Subject directly contact IZIX wanting to exercise their individual rights such as requesting a copy, correction or deletion of their data or wanting to restrict or object to the Processing activities, IZIX shall inform the Customer of such request within 2 business days and provide the Customer with full details thereof, together with a copy

of the Personal Data held by it in relation to the Data Subject, where relevant. IZIX shall promptly direct such Data Subject to the Customer. In support of the above, IZIX may provide the Customer's basic contact information to the requestor. The Customer agrees to answer to and comply with any such request of a Data Subject in line with the provisions of the applicable Data Protection Legislation.

6.3 Insofar as this is possible, IZIX shall cooperate with and assist the Customer by appropriate technical and organizational measures for the fulfilment of the Customer's obligation to respond to requests from Data Subjects exercising their rights.

7. DISCLOSURE

7.1 IZIX shall not disclose Personal Data to any Third Party, except in the following situations:

- 7.1.1 Where directed by the Customer;
- 7.1.2 As stipulated in the Agreement;
- 7.1.3 As required for Processing by approved Sub-processors in accordance with Article 10; OR
- 7.1.4 As required by law or regulatory authority, in which case IZIX shall inform the Customer of that legal requirement before disclosing that Personal Data, unless where applicable law prohibits such information being provided on important grounds of public interest.

7.2 IZIX represents and warrants that persons acting on behalf of IZIX and who are authorized to Process Personal Data or to support and manage the systems that Process Personal Data:

- 7.2.1 have committed themselves to maintain the security and confidentiality of Personal Data in accordance with the provisions of this DPA;
- 7.2.2 are subject to user authentication and log on processes when accessing the Personal Data; AND
- 7.2.3 have undertaken appropriate training in relation to Data Protection Legislation obligations.

7.3 IZIX shall inform the persons acting on its behalf about the applicable requirements and ensure their compliance with such requirements through contractual or statutory confidentiality obligations.

7.4 The Customer is subject to Protocol 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the European Union, particularly as regards the inviolability of archives (including the physical location of data and services as set out above and data security) which includes personal data held on behalf of the contracting authority in the premises of the Customer or subcontractor.

8. DELETION AND RETURN OF PERSONAL DATA

8.1 At the latest within 30 days upon termination of the Agreement, IZIX shall, at the discretion of the Customer, anonymize or destroy any Personal Data that it stores in a secure way that ensures that all Personal Data is anonymized or deleted and unrecoverable. Personal Data used to verify proper data processing in compliance with the assignment or that needs to be kept to comply with relevant legal and regulatory retention requirements may be kept by IZIX beyond termination or expiry of the Agreement only as long as required by such laws or regulations.

8.2 Upon written request submitted by the Customer no later than 14 calendar days prior to the termination or expiry of the Agreement, IZIX shall provide Customer with a readable and usable copy of the Personal Data and/or the systems containing Personal Data prior to anonymisation or destruction.

9. LOCATION OF PROCESSING

9.1 IZIX shall store Personal Data at rest within the territory of the European Economic Area (EEA).

9.2 Any Processing of Personal Data by IZIX personnel or subcontractors not located within the EEA may be undertaken only as provided by this DPA or following prior written approval of the Customer and the execution of one of the then legally recognized data transfer mechanisms, such as an additional data processing agreement governed by the Standard Contractual Clauses.

10. SUB-PROCESSING

10.1 The Customer acknowledges and expressly agrees that IZIX may use Third Party Sub-processors for the provision of IZIX Services as described in the Agreement.

10.2 Any such Sub-processors that provide services to and process Personal Data for IZIX shall be permitted to Process Personal Data only to deliver the services IZIX has entrusted them with and shall be prohibited from Processing such Personal Data for any other purpose. IZIX remains fully responsible for any such Sub-processor's compliance with IZIX's obligations under the Agreement, including this DPA.

10.3 IZIX shall, prior to the entrusting of services to a Sub-processor, carry out any relevant due diligence on such Sub-processor to assess whether it is capable of providing the level of protection for the Personal Data as is required by this Data Processing Agreement and provide evidence of such due diligence to the Customer where requested by the Customer or a regulator.

10.4 IZIX shall enter into written agreements with any such Sub-processor which contain obligations no less protective than those contained in this DPA, with respect to the protection of Personal Data to the extent applicable to the nature of the IZIX Services provided by such Sub-processor, including the obligations imposed by the Standard Contractual Clauses, as applicable.

10.5 Upon the Customer's written request, IZIX shall make available to the Customer the current list of Sub-processors for the provision of IZIX Services.

10.6 If the Customer objects to the use of a new Sub-processor that shall be processing the Customer's Personal Data, then the Customer shall notify IZIX in writing within 30 calendar days after being informed of the processing activities of said Sub-processor. In such a case, IZIX shall use reasonable efforts to change the affected Services or to recommend a commercially reasonable change to the Customer's use of the affected Services to avoid the Processing of Personal Data by the Sub-processor concerned. If IZIX is unable to make available or propose such change within 60 calendar days, the Customer may terminate the relevant part of the Agreement regarding those Services which cannot be provided by IZIX without the use of the Sub-processor concerned. To that end, the Customer shall provide written notice of termination that includes the reasonable motivation for non-approval.

11. TECHNICAL AND ORGANIZATIONAL MEASURES

11.1 IZIX has implemented and shall maintain appropriate technical and organizational measures intended to protect Personal Data or the systems that Process Personal Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss or destruction. These measures shall take into account and be appropriate to the state of the art, nature, scope, context and purposes of Processing and risk of harm which might result from unauthorized or unlawful Processing or accidental loss, destruction or damage to Personal Data. These measures shall always include the following measures:

- 11.1.1 the prevention of unauthorized persons from gaining access to systems Processing Personal Data (physical access control);
- 11.1.2 the prevention of systems Processing Personal Data from being used without authorization (logical access control);
- 11.1.3 ensuring that persons entitled to use a system Processing Personal Data gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing, Personal Data cannot be read, copied, modified or deleted without authorization (data access control);
- 11.1.4 ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);
- 11.1.5 ensuring the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed

from systems Processing Personal Data (entry control);

11.1.6 ensuring that Personal Data Processed are Processed solely in accordance with the instructions (control of instructions);

11.1.7 ensuring that Personal Data are protected against accidental destruction or loss (availability control);

11.1.8 ensuring that Personal Data collected for different purposes can be processed separately (separation control).

11.2 IZIX shall systematically adapt the technical and organizational measures to the development of regulations, technology and other aspects and supplement them with the applicable technical and organizational measures of Sub-processors, as the case may be. In any event, the implemented technical and organizational measures shall ensure a level of security appropriate to the risks represented by the Processing and the nature of the Personal Data to be protected, taking also into account the state of technology and the cost of their implementation.

11.3 Upon the Customer's written request, IZIX shall provide the Customer within 14 calendar days of receipt by IZIX of the Customer's request with a description of the implemented technical and organizational protection measures. An ISAE3402 type II report and/or other similar certifications can be used to describe and demonstrate compliance of the implemented technical and organizational measures.

12. DATA BREACHES

12.1 In the event of a (likely or known) Personal Data Breach and irrespective of its cause, IZIX shall notify the Customer without undue delay and at the latest within 48 hours after having become aware of (the likelihood or occurrence of) such Personal Data Breach, providing the Customer with sufficient information and in a timescale that allows the Customer to meet any obligations to report a Personal Data Breach under the Data Protection Legislation. Such notification shall as a minimum specify:

12.1.1 the nature of the Personal Data Breach;

12.1.2 the nature or type of Personal Data implicated in the Personal Data Breach, as well as the categories and numbers of Data Subjects concerned;

12.1.3 the likely consequences of the Personal Data Breach;

12.1.4 as the case may be, the remedial actions taken or proposed to be taken to mitigate the effects and minimize any damage resulting from the Personal Data Breach;

12.1.5 the identity and contact details of the Data Protection Officer or another Contact Person from whom more information can be obtained.

12.2 IZIX shall without undue delay further investigate the Personal Data Breach and shall keep the Customer informed of the progress of the investigation and shall take reasonable steps to further minimize the impact. Both Parties agree to fully cooperate with such investigation and to assist each other in complying with any notification requirements and procedures.

12.3 A Party's obligation to report or respond to a Personal Data Breach is not and shall not be construed as an acknowledgement by that Party of any fault or liability with respect to the Personal Data Breach.

13. AUDIT

13.1 IZIX makes available to the Customer all reasonable information, under the Agreement, to demonstrate compliance with its obligations laid down in this DPA or applicable Data Protection Legislation. IZIX notably allows and contributes to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, in accordance with this DPA.

13.2 If the information and reports provided by IZIX under this article are insufficient to allow the Customer to demonstrate that the obligations under the Data Protection Legislation are being met, the Parties will meet to agree on the operational, safety and financial terms of an on-site technical inspection. In any event, the conditions of this inspection must not affect the safety of the IZIX's other customers.

13.3 The Customer's information and audit rights exist only to the extent that the Agreement would not otherwise provide them with information and audit rights that meet the requirements of the applicable Data Protection Legislation. The Customer or the person mandated by the Customer to conduct an audit must inform IZIX or the relevant IZIX's partner of any audit or inspection to be conducted and makes (and ensures that each of the auditors commissioned make) every effort to avoid causing (or, if it cannot avoid, minimize) any damage, injury or disruption to the IZIX's premises, equipment, personnel and operations while the IZIX's personnel are on such premises during the course of such audit or inspection.

13.4 IZIX is not required to provide access to its premises for the purpose of such audit or inspection:

13.4.1 To an individual who does not have reasonable proof of identity and entitlement.

13.4.2 Outside normal business hours on its premises, unless the audit or inspection is to be carried out on an emergency basis and the Customer, or the person mandated by the Customer, has notified IZIX or the relevant partner of IZIX that the audit must be carried out before business hours.

13.5 If more than one audit or inspection occurs in a calendar year, additional fees may be invoiced to the Customer, except for additional audits or inspections where:

13.5.1 The Customer, or the person related to the Customer undertaking an audit, considers it reasonably necessary because of actual concerns about IZIX's, or the person related to the IZIX's, compliance with the DPA; or,

13.5.2 The Customer is required by data protection law, a data protection authority, or a similar regulatory authority responsible for the enforcement of data protection laws, to carry out this audit.

13.6 In addition, IZIX allows the Customer reasonable access to verify and/or audit IZIX compliance with the DPA, under the following conditions:

13.6.1 Any verification or inspection is limited to the processing activities and facilities directly involved in the processing of Personal Data;

13.6.2 The Customer gives IZIX reasonable written notice of at least 30 days prior to any audit or inspection (unless a shorter notice period is required by law, a regulatory authority or is otherwise agreed to by the Parties);

13.6.3 The Customer will conduct the audit or inspection during normal business hours and without creating a business interruption for IZIX, unless agreed with IZIX;

13.6.4 IZIX is not required to disclose or provide access to information relating to its own business activities or to third parties to whom IZIX has an obligation of confidentiality;

13.6.5 The audit or inspection is conducted in accordance with IZIX's relevant on-site policies and procedures, including, without limitation, those relating to access to premises, equipment, safety, health, security and data;

13.6.6 Where the audit or inspection is carried out by a third party on behalf of the Customer, such third party shall be bound by obligations equivalent to those set out in the DPA and may not be a competitor of IZIX;

13.7 The aforementioned on-site inspection, as well as the communication of certificates and inspection reports may result in a reasonable additional invoicing.

13.8 Notwithstanding the foregoing, the Customer is authorized to respond to requests from the competent supervisory authority provided that any disclosure of information is strictly limited to what is requested by the said authority. In such a case, and unless prohibited by applicable law, the Customer must first consult with IZIX.

13.9 In the event where (1) the audit requires the cooperation of a data hosting provider or other IT services provider, acting as a Sub-processor of IZIX and (2) that such Sub-processor is major company from which data processing agreements are not subject to negotiation with the Controller (e.g.: AWS, Microsoft Azure, OVH, etc.), the Customer expressly agrees that, insofar as such Sub-processor and its systems are concerned, the audit provisions enclosed in the data processing agreement from the Sub-processor shall be binding on the Customer and, consequently, opposable to the Customer. Such data processing agreement can be collected

directly from the Sub-processor or upon written request from the Customer.

14. CUSTOMER RESPONSIBILITIES

14.1 The Customer shall comply with all applicable laws and regulations, including the Data Protection Legislation.

14.2 The Customer remains responsible for the lawfulness of the Processing of Personal Data including, where required, obtaining the consent of Data Subjects to the Processing of their Personal Data.

14.3 The Customer shall take reasonable steps to keep Personal Data up to date to ensure the Personal Data are not inaccurate or incomplete with regard to the purposes for which they are collected.

14.4 With regard to components that the Customer provides or controls, including but not limited to workstations connecting to Services, data transfer mechanisms used, and credentials issued to the Customer's personnel, the Customer shall implement and maintain the required technical and organizational measures for protection of Personal Data.

15. NOTIFICATIONS

15.1 Unless legally prohibited from doing so, IZIX shall notify the Customer as soon as reasonably possible, and at the latest within 2 business days of becoming aware of the relevant circumstances, if it or any of its Sub-processors:

15.1.1 receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the Processing;

15.1.2 intends to disclose Personal Data to any competent public authority outside the scope of the Services under the Agreement. At the request of the Customer, IZIX shall provide a copy of the documents delivered to the competent authority;

15.1.3 receives an instruction that infringes the Data Protection Legislation or the obligations of this DPA;

15.2 IZIX shall co-operate as requested by the Customer to enable Customer to comply with any assessment, enquiry, notice or investigation under the Data Protection Legislation, which shall include the provision of:

15.2.1 Any and all data requested by the Customer (which is not otherwise available to the Customer) within the reasonable timescale specified by the Customer in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to the relevant Data Subject(s); AND

15.2.2 Where applicable, such assistance as is reasonably requested by the Customer to enable the Customer to comply with articles 32 to 36 of the GDPR and the relevant request within the Data Protection Legislation statutory timescales.

15.3 Any notification under this DPA, including a Personal Data Breach notification, shall be delivered to one or more of the Customer's Contact Persons via email possibly supplemented by any other means IZIX selects. Upon request of the Customer, IZIX shall provide the Customer with an overview of the contact information of the Customer's registered Contact Persons. It is Customer's sole responsibility to timely report any changes in contact information and to ensure Customer's Contact Persons maintain accurate contact information.

16. TERM AND TERMINATION

16.1 This DPA enters into force at the same moment as the Agreement and remains in force until Processing of Personal Data by IZIX is no longer required in the framework of or pursuant to the Agreement.

Last Update: 1 June 2024

ANNEXES TO APPENDIX I : DATA PROCESSING AGREEMENT

17. GENERAL

17.1 The following Annexes form an intergral part of the Appendix 1 : Data Processing Agreement to the Izix General Terms and Conditions.

ANNEX 1– SERVICES PROVIDED AND DETAILS OF PERSONAL DATA PROCESSED

PROCESSING ACTIVITIES	NATURE OF THE OPERATIONS CARRIED OUT AND PURPOSE OF DATA PROCESSING[1]	DATA SUBJECT [2]	TYPE OF DATA [3]	DATA RETENTION TIME [4]
Performance of Izix Services (parking access management through IZIX digital solution)	Creation and management of Customer's accounts	IZIX Customers	- Contract details (full name, first name, last name, email, phone number) ; - Languages ; - Licence Plate ; - Usage of Parking and bookings.	The data retention policy is the responsibility of the Data Controller.
	Management of parking access		- Contract details (full name, first name, last name) ; - Licence Plate ; - Usage of Parking and bookings.	
	Management of payments for Izix Services		- Contract details (full name, first name, last name, email) - Credit card details and holder ; - Address ; - Origin country.	

1 Operations carried out on the data (access, management, storage, etc.) = nature of the processing + Purpose for which the data is collected, recorded, processed, transmitted, stored, etc. = purpose
2 Aimed at persons whose personal data is processed in the context of subcontracting.
3 Any personal data of any kind processed in the context of the Subcontracting and the services provided by the Subcontractor to the Data Controller (which may include, in particular, identification data, financial data and sensitive data (in particular health data)).
4 The term of the Agreement (or a shorter term, depending on the nature of the services provided under the Agreement).

ANNEX 2 – AUTHORIZED SUB-PROCESSORS

Upon signature of the DPA, IZIX is authorized to use the following Sub-processors:

1. General Sub-Processors of Izix

NAME	Location	OUTSOURCED PROCESSING ACTIVITY
AWS (ISO27001)	EEC	Hosting and data center Services
Sentry	EEC	Logging and monitoring system Services
Mailjet	EEC	Transactional emails Services
Pusher	EEC	Real time notification system Services
Papertrail	EEC	Logging and monitoring system Services

2. Sub-Processors linked to specific Izix services.

NAME	Location	OUTSOURCED PROCESSING ACTIVITY
Stripe Payments Europe, Limited (SPEL)	ECC	Secure Payments Service Provider for the Prepaid Credit Feature
Aria Group (ISO27001)	Marocco	24/7 phone support for the Parking Desk service

ANNEX 3 - TECHNICAL AND ORGANIZATIONAL MEASURES

1 - Data center and network security

Physical security

1.1. Facilities: Izix servers are hosted on AWS at **SOC 2 Type II- and ISO 27001-compliant** facilities located within the borders of the European Union. In addition, the data center facilities are powered by **redundant power—each with UPS and backup generators**. Furthermore, hosting providers have **no access to customer data.**

1.2. On-site security: Our data center facilities are secured with a perimeter of multi-level security zones, 24/7 manned security, and CCTV video surveillance. In addition, they're secured via multi factor identification with biometric access control, physical locks, and security breach alarms.

Our office facilities are secured with nominative access control systems, CCTV surveillance. In addition, Wifi access points are password protected via strong passwords stored in keychains. Guest Wifi is provided to avoid strangers to connect to main Wifi. Automatic locking and password protection of computers is enforced globally.

1.3. Monitoring: An automatic monitoring system is in place to continuously check the state of the services, sending alerts to the appropriate personnel at Izix when necessary. Physical security, power, and internet connectivity are monitored by the facilities providers.

Network Security

1.4. Protection: Our network is protected by redundant firewalls, secure HTTPS transport over public networks, regular audits, and Intrusion Detection Systems (IDS) which monitor and/or block malicious traffic and network attacks.

1.5. Architecture: Our network security architecture consists of multiple security zones. More sensitive systems, like database servers, are protected in our most trusted zones that are not accessible from the public internet. Data transferred between Izix servers use a private network.

1.6. Third-party penetration tests: In addition to our extensive internal scanning and testing program, penetration tests are performed on a yearly basis. **1.7. Logical access:** Access to the Izix production network is restricted by an explicit need-to-know basis, utilizing least privilege. It is audited and monitored frequently, and controlled by our Management Team. Employees accessing the Izix production servers are required to use multiple factors of authentication when supported.

1.8. Security incident response: In case of a system alert, events are escalated to our 24/7 teams. Employees are trained on security incident response processes, including communication channels and escalation paths

Encryption

1.9. Encryption in transit: Communications between you and Izix servers are encrypted via industry best practices: HTTPS and Transport Layer Security 1.2 (or 1.3) (TLS) with an industry-standard AES-256 cipher over public networks. AES-256 is a 256-bit encryption cipher used for data transmission in TLS. Cryptographic keys protected by certificates, relying on the SHA256 signature algorithm. 1.**10. Encryption at rest:** The hard disks of all servers are encrypted thanks to an encrypted file system that encrypts all of your data and metadata at rest using an industry standard AES-256 encryption algorithm. Cryptographic keys protected by certificates, relying on the SHA256 signature algorithm.

Availability & Continuity

1.11. Redundancy: Izix employs service clustering and network redundancies to eliminate single points of failure. Our strict backup regime ensures customer data is actively replicated across geographically distinct data centers.

1.12. Disaster recovery: Our Disaster Recovery (DR) program ensures that our services remain available or are easily recoverable in the case of a disaster. This is accomplished by building a robust technical environment and creating disaster recovery plans that are continuously updated and tested.

2 - Application security

Secure development

2.1. Security training: Engineers participate in secure code training covering OWASP Top 10 security flaws, common attack vectors, and Izix security controls.

2.2. QA & Code Coverage: Our dedicated QA engineers test all software developments using automated and manual tests before roll-out to production. We strive to have very high code coverage across Izix applications.

2.3. Separate environments: Testing and staging environments are separated both physically and logically from the production environment.

2.4. CI/CD Deployment Process Izix uses the CI/CD (Continuous Integration, Continuous Deployment) deployment process. This plays a crucial role in maintaining high security standards thanks to Early Bug Detection, Automated Testing, Code Quality Control, Automated Security and Compliance checks and Rollback Mechanisms. This helps both ensuring the quality of deployed code as well as rapid response in case of issue.

2.5. Patches: Patches and updates to systems occur as needed following normal deployment constrains and procedures.

Application vulnerabilities

2.5. Static code analysis: The source code repositories are continuously scanned for security issues via our integrated static analysis tool. Any code change is scanned by these tools before hitting production as a standard procedure of our CI/CD release process.

2.6. Security penetration testing: Application security is also part of the annual penetration tests conducted by third-party experts.

3 - Product security features

Authentication security

3.1. Authentication options: Izix offers authentication options including username-password, SSO via Oauth and SAML2.0. Aim is to make Izix compatible with most SSO portals. Api and remote system can also connect using OAuth 2.0. Password data is always hashed and encrypted .Authentication method is defined by the customer for it's own Izix environment.

3.2. Secure credential management: When it comes to secure credential storage, Izix follows best practices: storing credentials in a password management system. Infrastructure components and Cloud systems are protected by strong password enforcement and short lived tokens.

3.3. API security & authentication: The Izix API is SSL-only. User or third party must be a verified user to make API requests. API access and authentication are possible via OAuth 2.0 protocols. In addition, user or third party needs to have the right authorizations and API scopes to be able to access customer data.

Additional product security features

3.4. Access rights & roles: Access to data within Izix is governed by access rights and can be configured to define granular access privileges. Izix has various permission levels for users (e.g. Admin, Reception, Security, Assistants, etc.).

3.5. Transmission security: All communications with Izix servers are encrypted using industry standard HTTPS and TLS 1.2 and 1.3 over public networks. This ensures that all traffic between you and Izix remains secure during transit.

3.6. Data segregation: Logical segmentation of customer data is enforced at code level effectively preventing data accessibility from one customer to another.

3.7. Data retention: You can automatically delete profiles after a given retention period, which allows you to comply more easily with privacy regulations such as the GDPR.

3.8. Audit trail: Audit trails including time of change and user responsible for the change are in place on critical objects.

3.9. Subprocessors: Izix carefully selects its third-party data Sub-processors and reviews them regularly. All such Sub-processors are contractually bound by Izix to keep customer data confidential.

3.10. JS injections prevention: To prevent JavaScript injections, we have implemented robust measures at the code level. Our approach includes rigorous input validation, content security policies that effectively restrict and control the resources the browser is allowed to load, training engineering personnel in secure coding practices.

4 - Compliance certifications, memberships, and external assessments

4.1. GDPR: Izix is in full GDPR compliance. Please refer to Privacy Policy and Data Processing Agreement.

4.2. SecurityScorecard: SecurityScorecard is an information security company that collects, attributes, and scores the overall health of enterprise cybersecurity through the identification of exposed vulnerabilities on corporate digital assets discovered on the public internet. Izix's score is A.

4.3. Level A: Our API and application endpoints are TLS/SSL-only. This means communications between you and Izix servers are encrypted via industry best practices: HTTPS and Transport Layer Security (TLS) over public networks.

5 - Additional security methodologies

4.4. Policies: Izix has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to all employees and contractors with access to Izix information assets.

4.5. Background checks: Izix performs background checks on all new employees in accordance with local laws. Criminal background checks are a part of these employee background checks. All newly-hired employees are screened through the hiring process and required to sign Non-Disclosure and Confidentiality Agreements.

4.6. Onboarding and Off boarding: Izix onboarding and off boarding policies ensure that access rights are given only after appropriate training is completed and the necessary security criteria have been achieved. Similarly, any sensitive access right is removed when an employee leaves the company or the project or immediately in case of gross negligence