

## XOPERO WHITEPAPER

# The security standards

Thanks to 256-bit algorithm encryption, two independent server localisations and unique combination of best-in-class physical security parameters we can guarantee the highest lever of data security.



AES 256 algorithm  
SSL certificate  
two localisations  
Briefcase  
data verification

### Data backup

- application encrypts data with AES 256 algorithm: the data is already encrypted on the user device and transmitted over the secure SSL protocol,
- data stored in two different locations: even in the event of failure of one of them user can still access the data,
- Briefcase application: encrypted on the user's device with a separate key, (different than the one used during backups), the key is generated automatically,
- files are divided into the smaller parts and then stored on the storage,
- data verification: during the sending process, application calculates the checksums for encrypted data and then, during restoring, it re-calculates checksums for all the data and compares them with each other.



default key  
user key  
AES 256 encryption

### Encryption

Xopero solutions use AES 256 CBC encryption (much stronger than regular AES 256 algorithm) and . Then SSL provides an additional level of security during the data transmission process. With AES 256 CBC every next block is encrypted using data from the previous element – that same process occurs during decryption. To provide the highest level of data security, users can choose a key (default or user) which will be used to encrypt transmitted data.

Default key is generated automatically during the first run of the application, so you do not have to worry about this key as it is stored in the data center. User is not able to lose this key, in any possible way,

User can also chose his own encryption key. It provides the maximum security of files because it is not stored anywhere, however in case of encryption key loss, the recovery of the encrypted data from the server is not possible.



data centers located in  
Europe and USA

### Secure data center

Our clients data is stored in one of our secure data centers located in USA or Poland. All data centers are purpose-built and located in the technology oriented areas. Facilities can accommodate the mission critical needs of leading technology companies and offer end-to-end capabilities to help enterprises build scalable, highly available, resilient, cost efficient and secure interconnected cloud environments to store data.

Unique combination of scale, best-in-class physical security parameters and market-leading energy efficiency.

- biometrics and key card access,
- at last two independent server localisations,
- UPS redundancy,
- emergency generators,
- close proximity to International Airports,
- limited exposure to risk of natural disasters.

All data centers meet the rigorous standards and compliance needs of global businesses. The following is a current list of some of the most valuable certifications and what they mean for our customers:

ISO/IEC 270001:2005 certificate in compliance with the PN-I-07799-2:2005 norm. Furthermore, the compliance certificate with the AQAP 2110:2006 norm, which defines requirements for military contracts and constitutes supplementation as well as extension of the already held ISO 9001:2000 quality certificate, was also granted. Furthermore, Unizeto Technologies data center received positive feedback after an audit according to WebTrust standard with respect to certification services connected with electronic signature (including SSL and EV SSL).



personal data  
protection

### Personal data protection

The protection of personal data is very important to us. In various situations, we may act have an personal data administrator or a personal data processor.

To provide our clients with the highest level of protection, we have implemented a number of tools to protect personal data, fully compliant with the high requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), i.e. "GDPR".

### Obligations related to the protection of personal data

In order to maintain high standards of personal data protection, we implemented the Personal Data Protection Policy as our internal document setting out the rules and procedures for the operation of personal data. In addition, if any personal data is entrusted to us, or we entrust it to other entities, it is done under the contracts for entrusting the processing of personal data, clearly defining the principles, responsibilities and scope of processing. In any case, our clients can be sure - personal data in our custody is safe.

We are the leading producer of backup solutions in Europe, providing professional tools for comprehensive backup of critical business data.

Our offer includes, among others appliance backup, local backup, cloud backup, hybrid backup and complex disaster recovery and business continuity solutions. Xopero products allow backup and recovery of files, folders, endpoints, databases, mailboxes, servers, network localizations and virtual environments.

Our customers belong to many different sectors: SMB, public administration, banking and finances, education, medicine, telecommunications and IT.