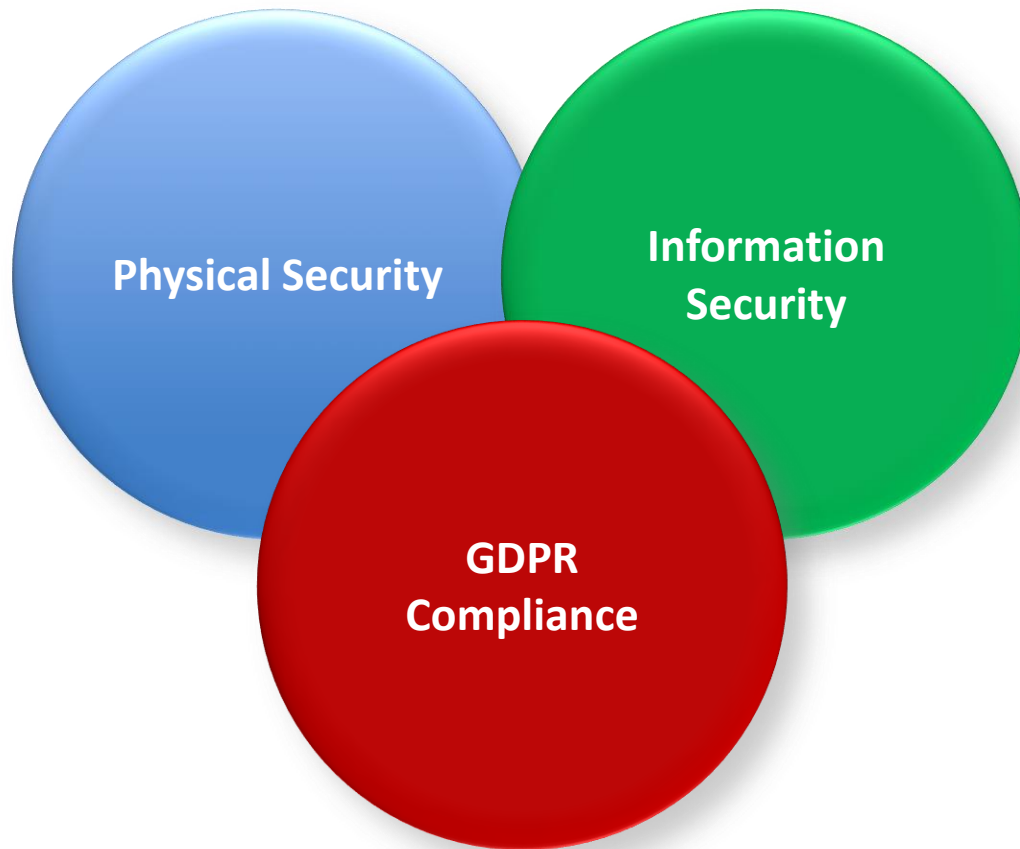


PAN EUROPEAN ROUTINES FOR MASTER KEY SYSTEMS DATA PROTECTION



INTRODUCTION AND BACKGROUND



INTRODUCTION AND BACKGROUND

Our intention

- To establish an agreed industry-wide process for protection of Master Key System related data, involving manufacturers, distributors and locksmiths

- To help our customers become GDPR compliant

- An initiative that covers the **complete MKS life cycle** from planning through calculation, production, delivery, installation and maintenance

INTRODUCTION AND BACKGROUND

- Master Key Systems are designed to support organizational requirements and to provide physical security in commercial and residential building applications.
- To prevent systems from being compromised, data security and information confidentiality are equally important as mechanical security.
- The European General Data Protection imposes new legal compliance requirements on manufacturers and distribution regarding protection of individuals' personal data.
- From planning through calculation, production, delivery, installation and maintenance (system life cycle) there is a defined chain of processes and interfaces that need to be considered concerning data security requirements and legal liability.
- The intention of the ARGE initiative is to establish an agreed industry-wide process for protection of Master Key System related data, involving manufacturers, distributors and locksmiths.

September 2018
ARGE MKS DATA PROTECTION INITIATIVE
16

SCOPE

1. Ordering and planning of cylinder systems
2. Transmission of lock-charts
3. General Data handling requirements
4. Calculation of Master Key Systems
5. Manufacturing of Master Key Systems
6. Shipment of Master Key Systems
7. Locksmith key cutting
8. Installation of Master Key Systems
9. Master Key Systems data lifetime management

ORDERING AND PLANNING

- **No personal data**
- **Neutral key marking**
- **Orders through authorized personnel**
- **GDPR risk assessment for electronic ordering and planning tools**
- **Order data processing agreements between locksmiths and suppliers**

ARGE

1. ORDERING AND PLANNING OF CYLINDER SYSTEMS

- Data to calculate and produce a Master Key System or a Key Alike System always has to be provided without personal data / information related to the individual key holders. Therefore key plans, org charts or any other documents / information provided to plan a system should always be created without showing any personal data (e.g. name, function, employee no., etc.).
- Key marking should avoid any obvious reference to its function, the location of the door and / or key holder.
- Suitable processes and security arrangements must be in place to ensure that orders for Master Key System keys and cylinders are only possible from authorized personnel.
- For electronic ordering and planning tools a GDPR successful risk assessment must be available to ensure legal compliance.
- Order data processing agreements must be in place between locksmiths and manufacturers / suppliers of MKS.

September 2018
ARGE MKS DATA PROTECTION INITIATIVE
19

TRANSMISSION OF DATA

- **MKS planning and ordering software using data encryption**
- **Encrypted transmission of data**
- **Hard copies transferred via registered mail or trackable courier service.**

2. TRANSMISSION OF LOCK CHARTS

- Electronic transmission of Lock Charts should use state of the art encrypted communication such as:
 - MKS Manufacturers' planning and ordering software with data encryption
 - Third party planning and ordering software with data encryption (software must meet data / GDPR protection and functional requirements as specified by MKS manufacturer)
 - email systems with encryption function enabled
- In cases where hard copy lock charts are required transfer should be via registered mail or trackable courier service.

```

graph LR
    EC([End Customer]) <--> L([Locksmith])
    L <--> M([MKS Manufacturer])
    M --> EC
            
```

September 2018
ARGE MKS DATA PROTECTION INITIATIVE
16

DATA HANDLING REQUIREMENTS

- **Definition of physical and electronic data protection**
- **Consideration of GDPR requirements**
- **Security screening for involved personnel**

3. GENERAL DATA HANDLING REQUIREMENTS

- Access management of secure server rooms and / or secure archives with paper files and / or security cards needs to be in place.
- Storage of electronic data needs to be in a secure file system or secure database environment.
- In cases where individuals' personal data is required, authorization for the use of the data must be provided by the individual and handling of the data must be GDPR compliant.
- Backup files must be created and protected.
- A matrix of roles and access permissions needs to be defined and continuously reviewed to maintain security procedures.
- Personnel with access to MKS calculation software and / or data need to be security screened / checked (e.g. Police Criminal Record) and be conversant with data protection- / GDPR requirements.
- Registration and storage of personnel's relevant data and documentation of access- rights and action logs is in line with GDPR as a legitimate business purpose during lifetime of the systems.

CALCULATION OF MASTER KEY SYSTEMS

- **Approved and GDPR compliant calculation SW only**
- **Specific rules for MKS calculations to ensure data security**

4. CALCULATION OF MASTER KEY SYSTEMS

- Calculation of MKS shall always be done using a calculation software tool which is either provided by the cylinder manufacturer (design owner) or third party calculation software that has been approved by the cylinder manufacturer.
- MKS calculations must always obey the specific rules defined by the cylinder manufacturers.
- Naming of calculations must not reference the location of the MKS.

MANUFACTURING OF MASTER KEY SYSTEMS

- **Restricted access to data and production of MKS to authorized persons only**
- **Test keys and incorrectly produced keys must be destroyed or kept in a secure environment**
- **No direct reference to installation sites**

5. MANUFACTURING OF MASTER KEY SYSTEMS

- Access to production / assembly area must be restricted to authorized persons only
- Access to assembly related paperwork or data must be restricted to authorized persons only. After use it must be destroyed / deleted or stored in a secure environment.
- Test keys and incorrectly produced keys must be destroyed or kept in a secure environment without direct reference to the location of the installation site.

SHIPMENT OF MASTER KEY SYSTEMS

- Security cards and Master Keys must be sent in sealed tamper-proof and non-transparent envelopes / enclosures
- Agree whether Security Card and Master Keys shall be included in MKS shipments or sent separately
- Shipments only with registered mail or trackable courier service

6. SHIPMENT OF MASTER KEY SYSTEMS

- Security cards and Master Keys must be sent in sealed tamper-proof and non-transparent envelopes / enclosures.
It shall be agreed between the manufacturer and the customer whether the Security Card and / or the Master Keys shall be included in MKS shipments or sent separately.
- Shipment of Master Key Systems, either complete or in part (cylinders and / or keys) must always be done using registered mail or trackable courier service.

September 2018
ARGE MKS DATA PROTECTION INITIATIVE
16

LOCKSMITH KEY CUTTING

- **Restricted access to key cutting machines**
- **Protected key blanks to be stored in secure and access controlled environment**
- **Records about protected key blank inventory covering cut keys, miss-cut keys and disposed keys.**

7. LOCKSMITH KEY CUTTING

- Access to key cutting machines must be controlled and limited to authorized personnel.
- Protected key blanks must be stored in a secure and access controlled environment.
- It is recommended to keep records about protected key blank inventory covering cut keys, miss-cut keys and disposed keys.

INSTALLATION OF MASTER KEY SYSTEMS

- **Authorized personnel only**
- **Key management**
- **Hand-over audits**
- **End-customer education**
- **Hand over of Security Cards, Master Keys and regular keys to be signed off by end-customers' authorized personnel.**

8. INSTALLATION OF MASTER KEY SYSTEMS

- Ensure that only authorized personnel has access to cylinders and keys during installation.
- Ensure that keys are not left in the doors after installation of cylinders.
- Conduct a hand-over audit to ensure all parts supplied and installed match with the order.
- Provide information about maintenance and service requirements to end-customer in order to maintain quality and security performance of the system.
- Hand over of Security Cards, Master Keys and regular keys must be signed off by end-customers' authorized personnel.

MKS DATA LIFE TIME MANAGEMENT

- **Any adjustments of MKS must be recorded in MKS log files**
- **Manufacturers and Locksmiths to keep records of card issuance, including new system cards, additional cards, replacement cards and lost cards**

9. MKS DATA LIFE TIME MANAGEMENT

- Any master key system produced and installed must record any adjustments in terms of system changes and / or extensions, replacement cylinders, re-codings, deleted cylinders, additional keys, deleted keys, system compromises and any other relevant information.
- The individual MKS log must include information about personnel involved in the different activities and the documentation of any activities described above.
- The purpose of Security Cards is to identify the master key system and to authorise re-ordering of cylinders and keys or key copies. Manufacturers and Locksmiths must keep records of card issuance, including new system cards, additional cards, replacement cards and lost cards.

CONCLUSIONS AND RECOMMENDATIONS

ARGE MKS Data Security Guideline

- Publish the content of the presentation as an agreed ARGE guideline on MKS Data Security to increase MKS security and achieve GDPR compliance
- Share new ARGE guidance with ELF to encourage the regional associations to adopt this within their members handbooks

Standardisation

- Incorporate most relevant elements of the guideline into the next revision of EN1303

GDPR Compliance

- ARGE to agree a template for a common data processing agreement that can be used between MKS manufacturers and distributors / locksmiths in order to achieve GDPR compliance

Common MKS Data Exchange Format

- Initiate a new ARGE working group with the aim of providing a (voluntary) common data structure for the exchange of MKS data.

THANK YOU