Richtlinie

Löschen von Informationen und Datenträgervernichtung

Guideline

Deletion of information and destruction of data carriers

Erstellt durch / Compiled by:

S. Giske

Stand / Version:

Rev. 01 / 11.12.2023

Inhaltsverzeichnis

Richtlinie - Löschen von Informationen und Datenträgervernichtung

Guideline - Deletion of information and destruction of data carriers

1. Einleitung

Diese Richtlinie befasst sich mit der Löschung von Informationen und der Vernichtung von Datenträgern. Unter dem Begriff Datenträger werden in dieser Richtlinie analoge Datenträger wie Papier oder Filme, sowie digitale Datenträger wie Festplatten, SSDs oder CDs zusammengefasst. Diese Richtlinie enthält darüber hinaus auch Regelungen für Smartphone, IoT-Devices und andere Geräte auf denen Informationen enthalten sein können.

Diese Richtlinie gilt für folgende Standorte der Kayser Automotive Gruppe:

A. Kayser Automotive Systems GmbH, Einbeck
A. Kayser Automotive Systems GmbH u. Co.KG, Glauchau
A. Kayser Automotive Systems Polska Spolka z o.o., Poznan
Kayser Automotive Systems Klodzko Sp. z o.o.
A. Kayser Automotive Ibérica, S.L. Automoción S. Com., Pamplona
Kayser Automotive Systems S en C., Puebla
Kayser Automotive Hungária Kft, Komárom
Kayser Automotive Systems (Changchun) Co., Ltd.
Kayser Automotive Systems USA, LP, Fulton

Diese Auflistung schließt eventuell vorhandene Außenstellen grundsätzlich mit ein. Abweichung von den Regularien dieser Richtlinie sind zu dokumentieren und zu begründen. Diese Richtlinie gilt für alle Mitarbeiterinnen und Mitarbeiter sowie für alle externen Dienstleister, die im Auftrag des Unternehmens Datenträger entsorgen oder vernichten.

2. Löschen von Informationen

2.1. Vorbereitung der Löschung

Bevor Informationen, unabhängig ihrer Form und auf welchem Medium, gelöscht werden, ist durch den für die jeweilige Information Verantwortlichen (Mitarbeiter) zu prüfen, ob eine Löschung der Information vorgenommen werden kann. Hierbei ist insbesondere zu prüfen, ob die zur Rede stehenden Informationen nicht einer gesonderten Aufbewahrungsfrist unterliegen. Dies ist im Einzelfall ebenso zu prüfen, wie die Frage ob die Informationen vor der Vernichtung eines

1. Introduction

This policy deals with the deletion of information and the destruction of data carriers. The term data carriers in this policy includes analogue data carriers such as paper or films, as well as digital data carriers such as hard disks, SSDs or CDs. This policy also contains regulations for smartphones, IoT devices and other devices that may contain information.

This policy applies to the following locations of the Kayser Automotive Group:

A. Kayser Automotive Systems GmbH, Einbeck
A. Kayser Automotive Systems GmbH u. Co.KG, Glauchau
A. Kayser Automotive Systems Polska Spolka z o.o., Poznan
Kayser Automotive Systems Klodzko Sp. z o.o.
A. Kayser Automotive Ibérica, S.L. Automoción S. Com., Pamplona
Kayser Automotive Systems S en C., Puebla
Kayser Automotive Hungária Kft, Komárom
Kayser Automotive Systems (Changchun) Co., Ltd.
Kayser Automotive Systems USA, LP, Fulton

This list fundamentally includes any existing branches. Deviations from the regulations of this policy are to be documented and justified. This policy applies to all employees as well as all external service providers who dispose of or destroy data carriers on behalf of the company.

2. Deletion of Information

2.1. Preparation for Deletion

Before information, regardless of its form and medium, is deleted, the person responsible for the respective information (employee) must check whether the information can be deleted. In particular, it must be checked whether the information in question is subject to a separate retention period. This must be checked on a case-by-case basis, as well as the question of whether the information can or must be transferred to another medium before the data carrier

Datenträgers auf ein anderes Medium übertragen werden können oder müssen. Handelt es sich bei den zu löschenden Informationen um personenbezogene Daten so sind datenschutzspezifische Regelungen (zum Beispiel Art. 17 EU-DSGVO, §75 BDSG, andere Vorschriften…) zu beachten. Im Zweifel ist der jeweilige Datenschutzbeauftragte zu involvieren.

2.2. Durchführung der Löschung / Vernichtung

Die Löschung und Vernichtung von Informationen ist je nach verwendetem Medium mittels eines, der Kritikalität der Informationen entsprechendes Verfahren durchzuführen. Die Entsorgung von Datenträgern muss so erfolgen, dass eine Wiederherstellung oder ein Zugriff auf die darauf gespeicherten Daten ausgeschlossen ist. Die Entsorgung von Datenträgern muss den Anforderungen an die Informationssicherheit und die Wahrung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit entsprechen.

Beim Einsatz von Dienstleistern sind die hier aufgeführten Anforderungen zum Vertragsbestandteil zu machen. Der Dienstleister ist als Informationssicherheitsrelevant zu klassifizieren. Im Wirkungskreis der EU-DSGVO ist darüber hinaus mit dem Dienstleister ein Auftragsverarbeitungsvertrag abzuschließen.

Folgende Anforderungen müssen für Information der Klassifikation „Intern“, „Vertraulich“ und „Streng Vertraulich“ mindestens eingehalten werden:

- Digitale wiederbeschreibbare Datenträger (z.B. USB-Sticks, Speicherkarten) müssen vollständig mit einem Datenstrom aus Zufallswerten (z. Bsp. PRNG Stream) überschrieben werden, wenn sie nicht verschlüsselt eingesetzt werden.
- Wenn digitale Datenträger verschlüsselt eingesetzt werden, müssen sie durch ein sicheres Löschen des Schlüssels gelöscht werden.
- Optische Datenträger (z.B. CD-ROM, DVD) müssen mindestens nach Sicherheitsstufe O-4 entsprechend der ISO/IEC 21964-2 vernichtet werden.

is destroyed. If the information to be deleted is personal data, data protection-specific regulations (for example Art. 17 EU-DSGVO, §75 BDSG, other regulations…) must be observed. If in doubt, the respective data protection officer should be involved.

2.2. Execution of Deletion / Destruction

The deletion and destruction of information must be carried out using a procedure appropriate to the criticality of the information, depending on the medium used. The disposal of data carriers must be carried out in such a way that recovery or access to the data stored on them is excluded. The disposal of data carriers must meet the requirements for information security and the preservation of the protection objectives of confidentiality, integrity and availability.

When using service providers, the requirements listed here must be made part of the contract. The service provider is to be classified as relevant to information security. Within the scope of the EU-DSGVO, a contract processing agreement must also be concluded with the service provider.

The following requirements must be met at least for information of the classification “Internal”, “Confidential” and “Strictly Confidential”:

- Digital rewritable data carriers (e.g. USB sticks, memory cards) must be completely overwritten with a data stream of random values (e.g. PRNG Stream) if they are not used encrypted.
- If digital data carriers are used encrypted, they must be deleted by securely deleting the key.
- Optical data carriers (e.g. CD-ROM, DVD) must be destroyed at least according to security level O-4 in accordance with ISO/IEC 21964-2.

- Smartphones oder sonstige Smart Devices sollten verschlüsselt werden. Smartphones oder sonstige Smart Devices müssen auf die Werkseinstellung (Factory Reset) zurückgesetzt werden. Anschließend muss der Einrichtungsvorgang zum Abschluss des Löschvorgangs durchgeführt werden.

- IoT Geräte müssen auf den Werkszustand zurückgesetzt werden. Sind die Geräte mit einem Clouddienst verbunden, so müssen diese vor dem Zurücksetzen aus der Cloudumgebung getrennt werden. Anschließend müssen alle in den IoT-Geräten hinterlegten Zugangsdaten geändert werden.

- Papier / Overheadfolien muss mindestens nach Sicherheitsstufe P-4 entsprechend der ISO/IEC 21964-2 vernichtet werden. Sollte es sich bei den Informationen um personenbezogene Daten im Sinne des Art. 9 EU-DSGVO (besonderer Kategorien personenbezogener Daten) handeln, so ist die nächsthöhere Sicherheitsstufe (P-5) bei der Vernichtung von Datenträgern zu wählen.

- In sonstigen Geräten integrierte Datenträger müssen über die integrierten Funktionen sicher gelöscht werden. Ist das nicht möglich, müssen die Massenspeicher ausgebaut und entweder wie herkömmliche digitale Datenträger von einem separatem IT-System aus sicher gelöscht werden oder mindestens nach Sicherheitsstufe E-4 bzw. H-4 entsprechend der ISO/IEC 21964-2 vernichtet werden.

2.3. Dokumentation der Löschung / Vernichtung

Jede Löschung von Informationen oder jeder Vernichtung eines Datenträgers muss in geeigneter Weise dokumentiert werden. Sofern ein Dienstleister hinzugezogen wurde, ist von diesem ein Vernichtungsnachweis in Form eines Protokolls anzufordern.

Dieses Protokoll sollte zumindest folgende Informationen enthalten:

- Art und Anzahl der Datenträger

- Smartphones or other smart devices should be encrypted. Smartphones or other smart devices must be reset to factory settings (Factory Reset). Afterwards, the setup process must be completed to conclude the deletion process.

- IoT devices must be reset to factory settings. If the devices are connected to a cloud service, they must be disconnected from the cloud environment before resetting. Afterwards, all access data stored in the IoT devices must be changed.

- Paper / overhead foils must be destroyed at least according to security level P-4 in accordance with ISO/IEC 21964-2. If the information is personal data within the meaning of Art. 9 EU-DSGVO (special categories of personal data), the next higher security level (P-5) must be chosen for the destruction of data carriers.

- • Data carriers integrated in other devices must be securely deleted using the integrated functions. If this is not possible, the mass storage devices must be removed and either securely deleted from a separate IT system like conventional digital data carriers or destroyed at least according to security level E-4 or H-4 in accordance with ISO/IEC 21964-2.

2.3. Documentation of Deletion / Destruction

Every deletion of information or every destruction of a data carrier must be documented in a suitable manner. If a service provider was involved, a certificate of destruction in the form of a protocol must be requested from them.

This protocol should contain at least the following information:

- Type and number of data carriers

• Seriennummer der vernichteten Datenträger (sofern vorhanden) • Datum und Ort der Vernichtung • Genutztes Verfahren (Sicherheitsstufe) • Name und Unterschrift des eingesetzten Mitarbeiters (kann auch in elektronischer Form vorliegen) • Bestätigung der ordnungsgemäßen Vernichtung der Informationen / Datenträger Die Dokumentation muss für mindestens 4 Jahre aufbewahrt werden, selbst dann, wenn nationale Regelungen eine kürzere Aufbewahrung erlauben.	• Serial number of the destroyed data carriers (if available) • Date and location of destruction • Procedure used (security level) • Name and signature of the employee used (can also be in electronic form) • Confirmation of the proper destruction of the information / data carriers The documentation must be kept for at least 4 years, even if national regulations allow for shorter retention.

Richtlinie - Löschen von Informationen und Datenträgervernichtung

Guideline - Deletion of information and destruction of data carriers

KAYSER AUTOMOTIVE SYSTEMS

Revision	Änderung / Change	Datum / Date	Ersteller / Author	Key-User	Prozessowner / process owner
01	Erstellung / Creation	11.12.2023	S.Giske	-	-