Informationssicherheitsstandard für Fremdfirmen

Inhaltsverzeichnis

1 Zweck

Informationen gehören zu den wichtigsten Vermögenswerten der Unternehmensgruppe Eberspächer („Eberspächer Gruppe“). Aufgrund der strategischen Bedeutung, die Informationen für die Eberspächer Gruppe haben, stellt deren Sicherheit ein Schlüsselfaktor bei der Zusammenarbeit mit externen Parteien dar. Die in diesem Dokument beschriebenen Regelungen haben zum Ziel, die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen der Eberspächer Gruppe sowie deren Rechte und Interessen im Hinblick auf Informationswerte zu schützen.

Dieser Standard beschreibt konkrete Anforderungen und Regelungen zum sicheren Umgang mit Informationswerten der Eberspächer Gruppe (im Folgenden auch: „Eberspächer“ oder „Auftraggeber“) und richtet sich an die Geschäftsführung von Fremdfirmen. Dazu zählen externen Lieferanten, Dienstleistern und sonstigen Partnern (im Folgenden auch: „Auftragnehmer“), deren Mitarbeiter sowie alle Drittparteien, die an der Erfüllung vertraglich vereinbarter Leistungen beteiligt sind.

2 Geltungsbereich

Dieses Dokument ist für alle genannten Auftragnehmer der Eberspächer Gruppe verbindlich.

Die beschriebenen Regelungen sind für alle Informationswerte der Eberspächer Gruppe anzuwenden. Neben elektronisch gespeicherten Informationen zählen hierzu insbesondere auch Unterlagen, Gespräche und Prototypen.

3 Definitionen/Benennungen/Abkürzungen

Auftragnehmer	Lieferanten, Dienstleister und Partner, die im Auftrag einer Gesellschaft der Eberspächer Gruppe vertraglich vereinbarte Leistungen erbringen.
GHV	Geheimhaltungsvereinbarung
Informations-verantwortliche/r	Informationsverantwortliche sind zuständig für die Klassifizierung einer Information, bestimmen den zulässigen Empfängerkreis und autorisieren Zugriffe (z.B. durch Vergabe/Genehmigung von Berechtigungen).
Sicherheitsniveau	Schutz gemäß der GHV und anerkannten Standards (z.B. Annex A der ISO/IEC 27001)

4 Umgang mit Informationswerten

4.1 Klassifizierung und Kennzeichnung von Informationswerten

Bei der Weitergabe, Übertragung, Aufbewahrung, Speicherung, Vernichtung und Löschung von Informationen sowie Informationsträgern des Auftraggebers ist die Vertraulichkeit zu wahren. Die Vertraulichkeit einer Information wird durch den/die Informationsverantwortliche/n des Auftraggebers anhand des nachfolgenden Schemas vorgegeben.

Die Klassifikation einer Information ist über ihren gesamten Lebenszyklus hinweg aufrechtzuerhalten und darf nur nach Freigabe durch den/die Informationsverantwortliche/n des Auftraggebers verändert werden.

Vertraulichkeit	Beschreibung
Öffentlich	Informationen, die für die Verwendung in der Öffentlichkeit bestimmt sind. **Lesender Zugriff:** Keine Einschränkung **Verändernder Zugriff:** Nach Freigabe **Löschender Zugriff:** Nach Freigabe **Verwendung in der Öffentlichkeit:** Nach Freigabe durch den Auftraggeber
Intern	Informationen, die für den internen Gebrauch (Mitarbeiter des Auftraggebers sowie befugte Auftragnehmer) bestimmt sind. Einschränkungen wie bei „Öffentlich“, ausgenommen: **Lesender Zugriff / Zugang:** Nur interne Mitarbeiter des Auftragnehmers, welche einen Zugriff zu den Informationen nach dem Need-to-know Prinzip benötigen; externe Mitarbeiter und Partner gemäß den Vorgaben der GHV. **Verwendung in der Öffentlichkeit:** Verboten **Schutzmaßnahmen:** Wirksamer Zugriffsschutz und Transportverschlüsselung. **Vernichtung:** Sichere Vernichtung der Informationen gem. Stand der Technik **Physische Sicherheit:** Beachtung der Vorgaben in Kapitel 4.5

Vertraulich	Informationen, die nur für die Verwendung durch definierte Personengruppen bestimmt sind. Einschränkungen wie bei „Intern“, ausgenommen: **Lesender Zugriff:** Nur definierte Personengruppen im Rahmen der Zusammenarbeit. Weitergabe an Dritte nur mit angemessenen Sicherheitsniveau oder Freigabe durch den Auftraggeber.
Streng vertraulich	Informationen, die nur für die Verwendung durch definierte Einzelpersonen bestimmt sind. Einschränkungen wie bei „Vertraulich“, ausgenommen: **Lesender Zugriff:** Nur definierte Einzelpersonen im Rahmen der Zusammenarbeit. **Schutzmaßnahmen:** Durchgängige sichere Verschlüsselung der Daten bei Übertragung (Ende-zu-Ende) und Speicherung. Wenn eine Verschlüsselung nicht möglich ist, müssen Informationen durch vergleichbar wirksame Maßnahmen geschützt werden.

„Streng vertrauliche“ Informationen müssen explizit als solche gekennzeichnet (z. B. Vertraulichkeitsvermerk) und mit besonderer Vorsicht behandelt werden.

Dem Auftragnehmer anvertraute Informationen sind, sofern keine davon abweichende Vereinbarung mit dem/der Informationsverantwortliche/n getroffen wurde, als *Vertraulich* zu behandeln.

4.2 Datenschutz

Die Erhebung und Verarbeitung von personenbezogenen Daten ist nur aufgrund einer Rechtsgrundlage zulässig. Im Falle einer Verarbeitung im Auftrag sind entsprechende vertragliche Regelungen zu vereinbaren, welche nähere Bestimmungen z. B. zu technischen und organisatorischen Schutzmaßnahmen treffen.

4.3 Schutz der Vertraulichkeit, Verfügbarkeit und Integrität

4.3.1 Zugriffsschutz

Der Auftragnehmer ist verpflichtet, die ihm durch den Auftraggeber anvertrauten Informationen mithilfe geeigneter Maßnahmen vor unbefugtem Zugriff (lesend, schreibend, löschend) zu schützen. Hierzu zählt eine Verschlüsselung nicht öffentlicher Informationen bei der Übertragung über öffentliche Netze.

Der Zugriff auf Informationswerte des Auftraggebers ist gemäß dem **„Need-To-Know“-Prinzip** einzuschränken, sodass nur diejenigen Personen Zugriff auf Informationen erhalten,

welche diesen für die Erledigung ihrer vereinbarten Aufgaben benötigen. Ein Zugriff durch den Auftragnehmer darf ausschließlich zweckgebunden im Rahmen der Aufgabenerfüllung erfolgen. Autorisierte Personen müssen zudem zur Geheimhaltung verpflichtet sein.

4.3.2 Umgang mit Zugangsdaten

Die Weitergabe von persönlichen Zugangsdaten (z. B. Passwörter, PINs, Zutrittsausweise), welche dem Zugriff auf Informationen des Auftraggebers dienen, ist verboten. Diese müssen stets sicher aufbewahrt werden.

Sofern Passwörter für den Zugriff auf Informationen des Auftraggebers verwendet werden, müssen diese aus mindestens acht Zeichen bestehen (zwölf Zeichen bei Konten mit administrativen Berechtigungen) und Zeichen aus mindestens drei der folgenden Kategorien enthalten:

- Großbuchstaben (A-Z*)
- Kleinbuchstaben (a-z*)
- Ziffern (0-9)
- Sonderzeichen
- Zeichen, die als Zeichen des Alphabets kategorisiert sind, jedoch weder zu den Groß- noch Kleinbuchstaben zählen. Insbesondere zählen hierzu Zeichen asiatischer Sprachen.

*Dazu zählen auch diakritische, griechische und kyrillische Zeichen.

Sofern PINs für den Zugriff auf Informationen des Auftraggebers verwendet werden, müssen diese aus mindestens sechs Ziffern bestehen.

Die Verwendung trivialer Zeichen- und Ziffernfolgen (z. B. 123456, abcd, 000000, etc.) und leicht zu erratender Zeichenfolgen (z. B. Namen, Jahreszahlen, Personalnummern, natürlichsprachliche Wörter etc.) in Passwörtern oder PINs ist nicht gestattet. Für verschiedene IT-Dienste und Anwendungen dürfen nicht die gleichen Passwörter und PINs verwendet werden.

Passwörter und PINs für den Zugriff auf Informationen und Systeme des Auftraggebers sind regelmäßig, spätestens jedoch nach sechs Monaten zu ändern. Alternativ sind kompensierende Maßnahmen (z.B. 2FA) zu definieren und nutzen. Diese dürfen nicht wiederverwendet werden und müssen sich zu Ihrem Vorgänger um mindestens drei Stellen unterscheiden.

4.3.3 Schutz der Verfügbarkeit von Informationen

Die Verfügbarkeit von Informationswerten des Auftraggebers muss seitens des Auftragnehmers durch geeignete Maßnahmen sichergestellt werden (z. B. regelmäßige Backups). Der permanente Verlust von Informationen oder Informationsträgern des Auftraggebers ist unverzüglich als Informationssicherheitsvorfall zu melden.

4.3.4 Weitergabe und Austausch von Informationen

Die Weitergabe/der Austausch („Weitergabe“) von nicht-öffentlichen Informationen des Auftraggebers im Sinne von 4.1 unterliegt den Regelungen der abgeschlossen GHV oder müssen dort ggf. zusätzlich geregelt werden.

Die Verarbeitung von nicht-öffentlichen Informationen des Auftraggebers in externen IT-Diensten (Cloud) ist gestattet, sofern durch den Auftragnehmer sichergestellt ist, dass der externe Dienst ein gleichwertiges Sicherheitsniveau bietet.

Sofern ein Informationswert beim Austausch nicht explizit gekennzeichnet ist, ist der Empfänger über die Klassifikation zu informieren.

I	HINWEIS
Für die Verarbeitung von personenbezogenen Daten gelten zusätzlich die Vorgaben in 4.2.	

4.4 Schutz von Soft- und Hardware

4.4.1 Bereitstellung

Sofern für die Aufgabenerfüllung benötigte Software oder Hardware durch den Auftraggeber bereitgestellt wird, ist diese vorrangig für die Speicherung und Verarbeitung von Informationen des Auftraggebers zu verwenden.

Informationen, die nicht im Zusammenhang mit der Aufgabenerfüllung stehen (z. B. private Informationen, Informationen von anderen Kunden) dürfen nicht auf bereitgestellten Geräten gespeichert oder verarbeitet werden.

Der Auftragnehmer ist für die ordnungsgemäße Nutzung der ihm zur Verfügung gestellten Soft- und Hardware im Rahmen seiner Aufgaben verantwortlich. Der Auftraggeber behält sich das Recht vor, die Bereitstellung jederzeit zu beenden.

4.4.2 Installation und Veränderung

Die Installation von Fremdsoftware auf durch Eberspächer bereitgestellten Geräten bedarf einer Freigabe durch den Auftraggeber. Die Deaktivierung von Schutzmaßnahmen (z. B. Deaktivierung des Virenschutzes) sowie die Veränderung der Betriebssystemkonfiguration ist auf bereitgestellten Geräten untersagt, sofern keine abweichenden Vereinbarungen getroffen wurden.

Durch den Auftraggeber bereitgestellte Firmware- und Software-Updates sind unverzüglich zu installieren.

Fremdgeräte (z. B. Laptops, Smartphones) dürfen nur nach schriftlicher Genehmigung des Auftraggeber mit dessen Netzwerke verbunden werden.

4.4.3 Schutz von Datenträgern

Beim Einsatz von mobilen Datenträgern ist darauf zu achten, dass immer nur die nötigsten Informationen gespeichert und nicht länger benötigte Informationen endgültig gelöscht werden.

Vertrauliche und streng vertrauliche Informationen sind grundsätzlich auf verschlüsselten Datenträgern zu speichern. Ausnahmen sind zuvor durch den Auftraggeber freizugeben.

4.4.4 Rückgabe und Löschung

Durch Eberspächer bereitgestellte und nicht mehr benötigte Geräte und Datenträger sind unverzüglich, spätestens aber bei Vertragsende, beim Auftraggeber zurückzugeben.

Auf Datenträgern des Auftragnehmers gespeicherte Informationen müssen bei Vertragsende vollständig an den Auftraggeber übergeben und anschließend sicher gelöscht werden. Vertraglich definierte und gesetzliche Aufbewahrungs- und Löschfristen sind hierbei einzuhalten.

4.5 Physische Sicherheit

Alle zur Verfügung gestellten Informationswerte (z. B. Dokumente, Prototypen) und Geräte sind gemäß ihrer Klassifizierung sachgemäß zu behandeln und vor Einsichtnahme durch Dritte, Verlust und Diebstahl zu schützen.

Überlassene Geräte und Informationen dürfen das Firmengelände des Auftraggebers nur mit Einwilligung des Auftraggebers verlassen.

Beim Verlassen des Arbeitsplatzes sind Geräte im laufenden Betrieb vor unbefugtem Zugriff zu schützen (z. B. passwortgeschützte Bildschirmsperre).

Es ist sicherzustellen, dass Geräte auf welchen nicht öffentliche Informationen des Auftragnehmers bearbeitet werden so aufgestellt werden, dass die Einsichtnahme unbefugten Dritten nicht möglich ist. Dies gilt sowohl innerhalb als auch außerhalb von Betriebsstätten.

Der Verlust von Informationswerten und Geräten des Auftraggebers ist unverzüglich zu melden. Dies gilt auch bei einem nur kurzfristigen Verlust, wenn der Zugriff Unbefugter nicht ausgeschlossen werden kann.

I	**HINWEIS**
Standortspezifische Regelungen zur physischen Sicherheit (z. B. besondere Schutzzonen, Fotografierverbot) sind vor Ort ausgewiesen und zu beachten.	

4.6 Meldepflichten

Der Auftragnehmer ist dazu verpflichtet, den Auftraggeber unverzüglich über Ereignisse und Risiken mit Relevanz für die Informationssicherheit in Bezug auf durch den Auftraggeber überlassene Informationen zu informieren.

Hierzu gehören u.a.:

- **Verletzung von Gesetzen, vertraglichen Regelungen und Vorgaben**
- **Informationssicherheitsvorfälle** (z. B. Verdacht auf Schadsoftwarebefall)
- **Datenschutzvorfälle** (z. B. Offenlegung personenbezogener Daten)
- **Identifizierte Risiken** (z. B. Schwachstellen in IT-Systemen)

*	**TIPP**
Für Fremdfirmen relevante Kontaktadressen für die Meldung von Ereignissen und Vorfällen in den Bereichen Informationssicherheit und Datenschutz sind im Kapitel 4.10 dieses Dokumentes zu finden.	

Der Auftragnehmer ist dazu verpflichtet, meldepflichtige Vorfälle in seinem Verantwortungsbereich zu dokumentieren, zu analysieren und durch geeignete Maßnahmen zu beheben.

Der Auftragnehmer ist darüber hinaus verpflichtet, nicht länger benötigte Berechtigungen (z. B. für IT-Systeme oder Zugangskontrollen) unverzüglich anzuzeigen.

4.7 Geistige Eigentumsrechte

Geistige Eigentumsrechte sind im Rahmen der Aufgabenerfüllung durch den Auftragnehmer zu wahren. Hierzu zählen z. B. Urheberrechte, Bildrechte oder Lizenzen.

Überlassene Softwarelizenzen dürfen nur für den vereinbarten Zweck und in Übereinstimmung mit der Lizenzvereinbarung des Herstellers verwendet werden. Der Einsatz von nicht-lizenzierter Software ist gemäß gesetzlichen Bestimmungen verboten.

4.8 Einhaltung der Vorgaben

Die Einhaltung der beschriebenen Vorgaben an die Informationssicherheit muss seitens des Auftragnehmers sichergestellt werden. Innerhalb der Organisation des Auftragnehmers sind zu diesem Zweck klare Verantwortlichkeiten für die Einhaltung und Umsetzung der beschriebenen Vorgaben zuzuweisen. Insbesondere sind Mitarbeiter des Auftragnehmers auf die Einhaltung der Informationssicherheitsvorgaben zu verpflichten.

Neben den in diesem Dokument spezifizierten Vorgaben sind im Rahmen der Aufgabenerfüllung relevante gesetzliche Anforderungen an den Daten- und Informationsschutz einzuhalten.

Sämtliche Informationssicherheitsvorgaben dieser Richtlinie sind auch für Unterauftragnehmer mit Zugriff auf Informationen des Auftraggebers verbindlich. Der Auftragnehmer ist dafür verantwortlich, die Einhaltung der Vorgaben bei Unterauftragnehmern sicherzustellen.

Die Nichteinhaltung oder Verletzung der vereinbarten Regelungen werden individuell nach betrieblichen und rechtlichen Vorschriften geprüft und entsprechend geahndet.

4.9 Überprüfung

Der Auftragnehmer ist dazu verpflichtet, die Einhaltung der relevanten Anforderungen und Vorgaben zur Informationssicherheit in seiner Organisation regelmäßig zu überprüfen. Weiterhin sind eventuelle Unterauftragnehmer ebenfalls einer regelmäßigen Prüfung zu unterziehen.

Die Eberspächer Gruppe behält sich darüber hinaus vor, die Einhaltung der Anforderungen und Vorgaben zur Informationssicherheit beim Auftragnehmer zu prüfen. Der Auftragnehmer ist dazu verpflichtet, die Überprüfung durch Bereitstellung von Selbstbeurteilungen („Self-Assessment“) sowie geeigneten Nachweisen zu unterstützen.

4.10 Kontakt

Für fachspezifische Fragen sowie zur Meldung von sicherheitsrelevanten Ereignissen, Vorfällen und Änderungen stehen folgende Kontaktmöglichkeiten zur Verfügung:

Ansprechpartner Informationssicherheit: informationsecurity@eberspaecher.com

Ansprechpartner Datenschutz: datenschutz@eberspaecher.com

5 Änderungshistorie

Stand	Erstellt/ geändert	Geprüft	Freigegeben	Bemerkung (geändert/hinzugefügt)
05	Dolde, Timo BLIIS 30.08.2024	Dolde, Timo BLIIS 30.08.2024	Peters, Martin BLI 30.08.2024	Document review
04	Dolde, Timo BLIIS 20.04.2022	Ade, Alexander BLI 20.04.2022	Peters, Martin B 20.04.2022	Schutzniveau definiert (Kap. 3). Informationen in 4 zum Umgang mit Informationen ergänzt. 4.1, 4.3.2 und 4.3.4 überarbeitet. Diverse Sätze präzisiert.
03	Halbach, Jonas BLIIS 03.05.2021	Ade, Alexander BLI 04.05.2021	Peters, Martin B 11.05.2021	Vollständige Überarbeitung des Dokuments Anpassung an aktuelle Vorgaben Entfernen aller Verlinkungen
02	Halbach, Jonas BPITE 10.12.2019	Schneider, Stefan BPITE 10.12.2019	Peters, Martin B 10.12.2019	Überarbeitung aufgrund von TISAX® Anforderungen Veröffentlichung als „Informationssicherheitsstandard“
01	Halbach, Jonas BPITE - Information Technology 31.07.2017	Melchior, Stefan BPI - Business Process & Information Management 31.07.2017	Peters, Martin B - Corporate Center 01.08.2019	Anpassung Passwortrichtlinie. Überarbeitung Kapitel 3.1 Anpassung an zentrales Dokumentenmanagement. Alter Name: BPI-S-ISF
BPI-S-ISF/00	Halbach, Jonas BPITE - Information Technology 28.09.2016	Vögele, Wolfgang BPITE - Information Technology 28.09.2016	Melchior, Stefan BPI - Business Process and Information Management 28.09.2016	Erstfreigabe