Datenschutz-Ordnung

Verantwortlich:	Geschäftsführung
Vertraulichkeitsstufe:	Interner Gebrauch
Vorgelagerter Prozess:	R018 Dokumentenlenkung
Nachgelagerter Prozess:	Verzeichnis der Verarbeitungstätigkeiten; siehe Punkt: „Ergänzende / weiterführende Dokumente“

Glossar

Betroffener / Betroffene Person	siehe: Personenbezogene Daten
Daten	Alle Daten im Unternehmen. Diese beinhaltet personenbezogene Daten und Unternehmensdaten.
Datenverarbeitungsanlage	Elektronische(s) Gerät(e), die für die Verarbeitung von personenbezogenen Daten genutzt werden. Dies sind z.B. Computer, Server, Notebook, Tablets, Netzwerkinfrastruktur.
Datenvorfall	Vorfall, bei dem der Schutz personenbezogener Daten verletzt wurde oder eine Verletzung vermutet wird bzw. möglich ist.
DSB	Datenschutzbeauftragter
DVA	Siehe Datenverarbeitungsanlage
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Unternehmensdaten	Alle Daten im Unternehmen ausgenommen der personenbezogenen Daten.
Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder .andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
Geschäftsführung	Zu der Geschäftsführung zählen Geschäftsführer und Prokuristen.

Datenschutz-Ordnung

1 Geltungsbereich (Verantwortlicher)

Hammer Schlüsseldienst Schröter + Fabian Haus für Sicherheit GmbH
Otto-Brenner-Str. 8
59067 Hamm Spezifische Verantwortlichkeit

2 Präambel

Diese Datenschutz-Ordnung enthält die grundsätzlichen Regelungen für den Umgang mit personenbezogenen Daten und zur Kontrolle der Einhaltung dieser Regelungen durch ein Datenschutz-Managementsystem. Sie soll das von europäischen und nationalen Regelungen, insbesondere der Europäischen Datenschutz-Grundverordnung (DS-GVO) und dem Bundesdatenschutzgesetz (BDSG) verlangte Datenschutzniveau und die Erfüllung der damit einhergehenden Rechenschaftspflichten gewährleisten.

Es ist für die Organe des Verantwortlichen wichtig,

- dass personenbezogene Daten ausschließlich im Rahmen der gesetzlichen Regelungen verarbeitet werden,
- dass die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz personenbezogener Daten nicht beeinträchtigt werden (Artikel 1 Abs. 2 DS-GVO),
- dass die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Artikel 5 Abs. 1 DS-GVO und die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO beachtet werden,
- dass die Rechte der Betroffenen insbesondere gemäß Kapitel III DS-GVO sichergestellt werden,
- und dass die Vorschriften zur Handhabung von Datenschutzverletzungen (Art. 33, 34 DS-GVO) eingehalten werden.

Die zuständigen Organe machen es sich zur Aufgabe dafür Sorge zu tragen,

- dass gemäß Artikel 24 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen ergriffen werden und der Nachweis erbracht werden kann, dass die Verarbeitung personenbezogener Daten den Vorgaben der DS-GVO folgt,
- dass die technische Umsetzung der Verarbeitung personenbezogener Daten den Prinzipien Privacy by Design und Privacy by Default (Artikel 25 DS-GVO) Rechnung trägt,
- und dass geeignete technische und organisatorische Maßnahmen getroffen, geprüft und mit dem Stand der Technik regelmäßig weiterentwickelt werden, um den Verpflichtungen von Artikel 32 DS-GVO gerecht zu werden.

3 Weitere Dokumente

Diese Datenschutz-Ordnung wird durch weitere Dokumente, z.B. Verfahrensbeschreibungen, technische und organisatorische Maßnahmen, Richtlinien und Prozessbeschreibungen, ergänzt (siehe „Ergänzende / weiterführende Dokumente“).

4 Umfang und Verwendung der zu verarbeitenden Daten

Bei dem Verantwortlichen werden Unternehmensdaten und personenbezogene Daten von Kunden, Beschäftigten des Unternehmens, der Lieferanten sowie weiterer Geschäftskontakte verarbeitet.

Es dürfen nur personenbezogene Daten erhoben und verarbeitet werden, wenn der Betroffene in die Datenverarbeitung eingewilligt hat oder eine gesetzliche Norm die Datenverarbeitung vorschreibt.

5 Zweckbindung

Die Datenverarbeitung hat zweckgebunden zu erfolgen. Die Zwecke der Datenverarbeitung personenbezogener Daten sind auf den Geschäftszweck begrenzt und in dem *Verzeichnis der Verarbeitungstätigkeiten* beschrieben.

6 Schutzbedarf der Daten

Der Schutzbedarf der Daten richtet sich nach der Datenkategorie. Diese ist dem *Verzeichnis der Verarbeitungstätigkeiten* zu entnehmen.

Besondere Kategorien personenbezogener Daten sind gem. Art. 9 (1) EU Datenschutz Grundverordnung (kurz. EU DSGVO) sind Informationen über:

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugung
- Gewerkschaftszugehörigkeit
- Gen-Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zum Sexualleben oder sexuellen Orientierung

einer natürlichen Person. Diese Daten unterliegen einem höheren Schutzbedarf.

Ebenso haben Informationen über

- Bankverbindung
- Kreditkarten
- Zugangsdaten für Alarmanlagen
- Informationen zu Schließsystemen (z.B. Schlüsselherstellungsdaten, Schneiddaten, Daten elektronischer Schlösser)

einen höheren Schutzbedarf.

7 Einhaltung von Datensparsamkeit und Datenvermeidung

Es sollen nur die Daten verarbeitet werden, die für die Erfüllung der unternehmerischen Aufgaben erforderlich sind und im Einklang mit den datenschutzrechtlichen Bestimmungen stehen. Hierbei ist darauf zu achten, dass nur so wenige Daten wie nötig erhoben, verarbeitet und genutzt werden.

Nicht mehr erforderliche bzw. genutzte Daten sind zu sperren bzw. zu löschen. Hierbei sind die gesetzlichen Aufbewahrungs- und Löschfristen zu beachten.

8 Rechte von betroffenen Personen

Der Betroffene ist die Person, deren personenbezogenen Daten bei dem Verantwortlichen verarbeitet werden.

Jeder Betroffene kann die folgenden Rechte geltend machen:

- Auskunft
- Berichtigung
- Widerspruch gegen die Datenverarbeitung
- Löschung von personenbezogenen Daten
- Einschränkung der Verarbeitung
- Datenübertragbarkeit

Macht ein Betroffener von einem der oben genannten Rechte gebrauch, so ist die Richtlinie *R003 Anfrage eines Betroffenen* zu beachten.

Bevor die Rechte des Betroffenen umgesetzt werden, muss die Identität des Betroffenen zweifelsfrei festgestellt (Authentifizierung des Betroffenen) werden.

9 Verzeichnis der Verarbeitungstätigkeiten

Das *Verzeichnis der Verarbeitungstätigkeiten* setzt sich aus verschiedenen *Verfahrensbeschreibungen* zusammen.

In der Verfahrensbeschreibung wird die Datenverarbeitung beschrieben und dokumentiert. Sie umfasst mindestens:

- Name und Kotaktdaten des Verantwortlichen

- Verantwortlicher für das Verfahren
- Zwecke der Verarbeitung
- Kategorien der personenbezogenen Daten
- Kategorien der Betroffenen
- Kategorien von Empfängern
- Übermittlung von Daten (insbesondere Drittland-Übermittlung)
- Löschfristen
- Technische und organisatorische Maßnahmen

Der *Verantwortliche für das Verfahren* erstellt die Verfahrensbeschreibung und ist für die regelmäßige (mindestens jährliche) Prüfung und Aktualisierung selbiger verantwortlich.

Der *Datenschutzbeauftragte* kann zur fachlichen Unterstützung hinzugezogen werden.

Der *Verantwortliche für das Verfahren* ist grundsätzlich die Geschäftsführung. Sollte abweichend von dieser Regelung eine andere Person für das Verfahren verantwortlich sein, legt sie eine neue oder geänderte Verfahrensbeschreibung der *Geschäftsleitung* zur Genehmigung vor.

Der *Datenschutzbeauftragte* nimmt die genehmigten Verfahrensbeschreibungen in das *Verzeichnis der Verarbeitungstätigkeiten* auf.

10 Datenschutzfolgenabschätzung

Die Datenschutzfolgenabschätzung ist durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Ein hohes Risiko für die Rechte und Freiheiten des Betroffenen liegt insbesondere dann vor, wenn
- Besondere Kategorien von personenbezogenen Daten
- Daten von Bankverbindungen
- Kreditkartendaten
- Bilder einer Videoüberwachung

verarbeitet werden oder wenn die technischen Maßnahmen für den Schutz der Daten nicht ausreichend oder mangelhaft sind.

Bevor eine neue Datenverarbeitung (z.B. Software) betrieben wird oder eine bestehende geändert wird, die ein hohes Risiko für die Rechte und Freiheiten von Betroffenen (siehe oben) darstellen könnte, muss die Datenschutzfolgenabschätzung durchgeführt werden.

Der *Datenschutzbeauftragte* wird von dem *Verantwortlichen* oder dem *Verantwortlichen für das Verfahren* im Voraus informiert. Der *Datenschutzbeauftragte* kann beratend hinzugezogen werden.

11 Vermeidung von Rechtsverletzung und Ihrer Folgen

Personen, die im Unternehmen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, werden mindestens einmal jährlich zu datenschutzrelevanten Themen und zum sachgemäßen und rechtskonformen Umgang mit personenbezogenen Daten geschult. Die Beschäftigten sind durch den Datenschutzbeauftragten und ggf. weitere qualifizierte Personen bzw. Einrichtungen zu schulen. Die Schulungsteilnahme ist schriftlich oder in Textform nachzuweisen. Die Nachweise werden vom *Geschäftsführung* verwaltet. Die Schulung kann als Präsenzschulung oder Webinar erfolgen.

Neue Beschäftigte sind durch eine Webinar-Schulung initial im Datenschutz zu unterweisen. Ihnen ist diese *Datenschutz-Ordnung* auszuhändigen oder in anderer geeigneter Weise zur Verfügung zu stellen. Sie sind auf die Vertraulichkeit im Umgang mit personenbezogenen Daten und Unternehmensdaten durch die *Geschäftsführung* zu verpflichten.

Tatsächliche und vermutete Datenvorfällen, Datenschutzverletzungen oder Datenpannen sind durch den Beschäftigten entsprechend der Richtlinie *R0001-Datenvorfall* zu melden.

Ist der Beschäftigte unsicher im Umgang mit Daten, so hat er sich an seinen Vorgesetzten oder den *Datenschutzbeauftragten* zu wenden.

Beschäftigte dürfen nur Software (Applikationen, Apps) installieren, die durch die *Geschäftsführung* genehmigt wurde.

Vor dem Ende eines Beschäftigungsverhältnisses ist der ausscheidende Beschäftigte durch die *Geschäftsführung* zu belehren, dass die Vertraulichkeitsverpflichtung auch über das Ende der Beschäftigung hinweg gültig ist. Nach Möglichkeit sollte die Belehrung direkt nach Aussprache der Kündigung vorgenommen werden. Die Belehrung ist zu dokumentieren.

12 Regelung der Verantwortlichkeit im Datenschutz

Die *Geschäftsführung* ist für die Umsetzung der Datenschutzregelungen und -gesetze sowie für die Einhaltung dieser Datenschutz-Ordnung verantwortlich und stellt dies mit der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen sicher. Insbesondere ist sie für die Durchführung der *Datenschutzfolgenabschätzung* und *Auftragskontrolle* verantwortlich.

Der *Geschäftsführung* ist für die technische Umsetzung der erforderlichen Maßnahmen in seinem Aufgabengebiet (insbesondere der Datenverarbeitungsanlagen) verantwortlich. Dies sind insbesondere Patch-Management, Datensicherung, Verbindungssicherheit, Härtung der Systeme.

Die Geschäftsführung ist für die Vertraulichkeitsverpflichtungen der Beschäftigten und deren Nachweis verantwortlich.

Der *Datenschutzbeauftragte* unterrichtet und berät den Verantwortlichen und seine Beschäftigten hinsichtlich ihrer Pflichten nach der EU Datenschutz Grundverordnung (EU DSGVO) und sonstigen Datenschutzvorschriften. Er überwacht die Einhaltung der EU DSGVO und anderer Datenschutzvorschriften. Er berät – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung. Der Datenschutzbeauftragte ist Ansprechpartner für Beschäftigte, Betroffene und die Aufsichtsbehörden.

Der *Datenschutzbeauftragte* ist bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung und Vertraulichkeit gebunden (Art.38 (5) EU DSGVO).

Jeder Beschäftigte ist für den Datenschutz in seinem Arbeitsbereich und für die ihm fachlich oder disziplinar unterstellten Beschäftigten für die Umsetzung des Datenschutzes verantwortlich.

Jeder Beschäftigte hat die Möglichkeit und die Pflicht sich bei Fragen zum Datenschutz an den *Datenschutzbeauftragten* zu wenden

Jeder Beschäftigte erteilt dem *Datenschutzbeauftragten* die erforderlichen Auskünfte.

Bei tatsächlichen oder vermuteten Angriffen auf das Netzwerk von Innen oder Außen (hierzu zählen auch Computerviren, Trojaner, Schadsoftware) sind die Regelungen der *Richtlinie R001 Datenvorfall* zu beachten.

13 Auftragsverarbeitung

Soll ein Auftragnehmer beauftragt werden und werden diesem personenbezogene Daten zur Verfügung gestellt oder dieser könnten personenbezogene Daten einsehen, so muss vor der Beauftragung ein Vertrag zur Auftragsverarbeitung geschlossen werden. Vor der geplanten Beauftragung informiert, der entsprechende Fachbereich die *Geschäftsführung*. Nach Maßgabe der *Geschäftsführung* wird der *Datenschutzbeauftragten* einbezogen und führt die erforderliche Prüfung des Auftragnehmers durch.

Die *Geschäftsführung* ist dafür verantwortlich, dass Auftragsdatenverarbeitungen vertraglich gem. Art. 28 EU DSGVO in Schriftform oder elektronisch vereinbart werden. Der *Datenschutzbeauftragte* unterstützt dies fachlich.

Ist das Unternehmen (im Sinne von Art. 28 EU DSGVO) Auftragnehmer einer V*erarbeitung im Auftrag*, so ist die *Geschäftsführung* dafür verantwortlich, dass die Beschäftigten entsprechend den Weisungen des *Auftraggebers* unterwiesen werden und dass die diesbezüglichen Informations- und Meldepflichten eingehalten werden.

14 Besonderheiten einer Datenverarbeitung in Drittländern

Die Daten sollen vorrangig in Deutschland verarbeitet werden. Die Datenverarbeitung in Ländern außerhalb der EU ist nicht gestattet.

15 Allgemeine technische und organisatorische Maßnahmen

Unbefugten ist der Zutritt zu Räumen mit Datenverarbeitungsanlagen (kurz: DVA) zu verwehren. Diese Räume und deren Fenster sind durch dem *Beschäftigten* zu verschließen und die Alarmanlage zu aktivieren, der ihn als letzter verlässt. Betriebsfremde sind in einem Besprechungsraum zu empfangen. In Ausnahmefällen ist Betriebsfremden der Zutritt zu den Arbeitsbereichen in Begleitung von Beschäftigten gestattet, wenn sichergestellt werden kann, dass keine Einsicht in schützenswerte Daten erfolgen kann.

Durch geeignete Maßnahme ist sicherzustellen, dass Beschäftigte nur auf die Daten zugreifen können, die sie für die Erfüllung ihrer Aufgaben benötigen (need-to-know-Prinzip).

Schützenswerte Daten – insbesondere personenbezogene Daten – müssen auf dem Transportweg gegen die Einsichtnahme durch Dritte geschützt werden. Hierzu sind gängige Verschlüsselungsmechanismen und –Techniken zu nutzen.

Die Technischen und organisatorischen Maßnahmen (kurz: TOM) sind im Dokument *VVT002 Allgemeine technische und organisatorische Maßnahmen* beschrieben.

16 Protokollierung

Im Rahmen der Sicherstellung der Datensicherheit werden Netzwerktransportdaten sowie Daten der Betriebssystem- und Netzwerksicherheit protokolliert. Diese Protokollierung dient Datenschutzkontrolle, der Datensicherheit, der Datensicherung und der Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlagen bzw. dem Nachweis von Datenschutzverstößen sowie der Strafverfolgung bei illegalen Handlungen oder Handlungen, die gegen diese Datenschutz-Ordnung verstossen.

17 Veröffentlichungen (im Internet)

Die Veröffentlichung von personenbezogenen Daten ist nur mit Einwilligung des Betroffenen gestattet. Unternehmensbezogene Daten dürfen nur mit Zustimmung der *Geschäftsführung* veröffentlicht werden. Diese Regelungen gilt auch, wenn Beschäftigte im Rahmen Ihres Privatlebens Veröffentlichungen im Internet vornehmen.

Der *Datenschutzbeauftragte* prüft die Internetseite(n) des Verantwortlichen nach dessen Maßgabe. Für jede Internetseite ist eine Datenschutzerklärung durch den *Verantwortlichen* oder auf Weisung der *Geschäftsführung* durch den *Datenschutzbeauftragten* zu erstellen. Durch einen geeigneten Rechtsanwalt sind die rechtlichen Anforderungen an die Internetseite – insbesondere Informationspflichten - zu prüfen.

18 Ausnahmen

Jede Ausnahme von den oben genannten Anforderungen muss durch die *Geschäftsführung* schriftlich oder in Textform genehmigt werden.

19 Ergänzende / weiterführende Dokumente

Dokument	Beschreibung
R001 Datenvorfall	Zu ergreifende Maßnahmen im Falle eines Datenvorfalls
H012 Meldung Datenvorfall	Formular zur Meldung eines Datenvorfalles
R002 Aufsichtsbehörde	Zu ergreifende Maßnahmen bei Anfragen durch die Aufsichtsbehörde
R004 Passwortrichtlinie	Regelung zur Gestaltung und Verwendung eines Passwortes

R005 Beteiligung des Datenschutzbeauftragten	Maßnahmen zur Beteiligung des Datenschutzbeauftragten
R007 Datensicherungsrichtlinie	Regelung zur ordnungsgemäßen Durchführung der Datensicherung
Verlust von Hardware	Der Verlust von Hardware und die darauf folgenden Maßnahmen sind in der Richtlinie *R001 Datenvorfall* beschrieben.
R009 Private Internetnutzung	Regelungen zum Umfang der privaten Nutzung der betrieblichen Internetverbindung
H015 Vereinbarung private Nutzung	Formblatt zur für die Vereinbarung zur privaten Nutzung von Internet / Email
R011 Private Nutzung	Regelungen zur privaten Nutzung von betrieblichen Datenverarbeitungsanlagen
R012 Einsichtnahme von User-Account	Zu ergreifende Maßnahme, wenn ein User-Account oder ein Emailpostfach eingesehen werden sollen.
R013 Home Office	Maßnahme und Regelung für Mitarbeiter, die im Home-Office (zeitweise) arbeiten.
R015 Richtlinie Emailnutzung	Regelungen zur Nutzung der betrieblichen Emailadresse.
R0016 Clean Desktop	Regelungen zur Ordnung am Arbeitsplatz
R019 Datenträgervernichtung	Entsorgung und Vernichtung von Datenträgern (Papier, Festplatten, CD-ROM etc.)
R022 Verschlüsselung	Regelung für die Sicherung von Daten auf dem Transportwege.

20 Änderungs-Historie

Datum	Erstellt durch	Genehmigt durch	Beschreibung der Änderung
06.07.2019	Haye Hösel	Markus Ciminski	Erstellung