exkulpa

Datenschutzmanagement und Prozessbeschreibungen

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

Datenschutz-Management der Firma XY GmbH

[Firmenlogo]

Stand: tt.mm.2020

Übersicht

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de

I. Selbstverpflichtung zum Datenschutz

In unserem Unternehmen genießt der Datenschutz unter Einbeziehung personenbezogener und anderer vertraulicher Daten höchste Priorität.

Im Rahmen unserer Geschäftstätigkeit werden regelmäßig und unvermeidbar schutzwürdige Daten erhoben, verarbeitet, genutzt und anderen Personen zur Verfügung gestellt.
Dabei wird das Maß der Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter Beachtung datenschutzrechtlicher Zulässigkeitsvoraussetzungen auf das notwendige Minimum zur Aufgabenerfüllung begrenzt.

Eine Verarbeitung und Nutzung personenbezogener Daten erfolgt nur, wenn eine Rechtsgrundlage einschlägig ist oder mit (schriftlicher) Einwilligung des Betroffenen oder ist im Geschäftsinteresse dann zulässig, wenn das schutzwürdige Interesse des Betroffenen nicht gegenüber dem Beschluss der Verarbeitung oder Nutzung überwiegt.
Unsere Mitarbeiter sind über die einschlägigen Datenschutzvorschriften belehrt. Jährlich werden sie durch den Datenschutzbeauftragten über Änderungen und Aktualisierungen im Datenschutzrecht geschult. Die Verpflichtungen der Mitarbeiter auf den Datenschutz sind aktenkundig.
Jeder Mitarbeiter ist sich dessen bewusst, dass ihm anvertraute personenbezogene Daten ausschließlich im Rahmen der Zweckbestimmung verwendet werden und gegen unberechtigten Zugriff gesichert werden müssen.
Teil unseres Verständnisses von Datenschutz ist es, dass

- ausschließlich vom Unternehmen freigegebene Softwareverfahren angewendet werden,
- keine Veränderungen an der Hard- und Software vorgenommen werden,
- keine eigene Hard- und Software eingesetzt werden darf und
- alle unternehmenseigenen Richtlinien und Maßnahmen von allen Mitarbeitern, Leiharbeitnehmern, Fremdfirmen und Besuchern

eingehalten werden.

Daten und Programme müssen vor unbefugter Einsichtnahme, vor Datendiebstahl oder -verlust zuverlässig geschützt werden. Die Mitarbeiter des Unternehmens verpflichten sich, hierfür größtmögliche Sorgfalt walten zu lassen.

Wir arbeiten mit aktualisierten Daten. Nicht mehr benötigte Daten werden zuverlässig gelöscht. Fehlerhafte Angaben werden zeitnah berichtigt. Bei der Archivierung von Daten wird eine weitere Nutzung dieser Daten ausgeschlossen. Gesetzliche Aufbewahrungsfristen bzw. Archivierungsfristen werden eingehalten. Es werden grundsätzlich nur die zur Erfüllung gesetzlicher, vertraglicher oder vorvertraglicher Zwecke unbedingt notwendigen personenbezogenen Daten archiviert.

Gemäß gesetzlicher Vorgabe hat jeder Beschäftigte das Recht auf Auskunft über die Verarbeitung seiner personenbezogenen Daten, das Recht, die seine Person betreffenden Daten einzusehen, sie ggf. berichtigen, sperren oder löschen zu lassen, soweit kein berechtigtes Interesse seitens des Unternehmens in Bezug auf diese Daten besteht oder gesetzliche Aufbewahrungspflichten dem Entgegenstehen.

Das Unternehmen verpflichtet sich, vor erstmaliger Verarbeitung personenbezogener Daten den Betroffenen zu informieren.

Das Unternehmen hat einen Datenschutzbeauftragten schriftlich bestellt. Zur Umsetzung datenschutzrechtlicher Forderungen im Unternehmen besitzt er gegenüber der Geschäftsleitung ein direktes Vortrags-, Empfehlungs- und Beratungsrecht. In der Anwendung seiner Fachkunde ist er weisungsfrei.

Mitarbeiter haben jederzeit das Recht, den Datenschutzbeauftragten (auch anonym) zu Fragen des Datenschutzes und zu Fragen mit der Verarbeitung sie betreffender Daten zu kontaktieren. Der Datenschutzbeauftragte unterliegt diesbezüglich der Vertraulichkeit und der Verschwiegenheit.

II. Datenschutz-Team & Verantwortliche für den Datenschutz		
Unternehmen	Firma XY GmbH, Anschrift	evtl. Niederlassungen und sonstige (Tochter-) Gesellschaften, die von der DSB-Betreuung umfasst sind
Verantwortlicher	Name der Geschäftsleitung	
Datenschutz-beauftragter (DSB)	Name und Kontakt	Wirkt auf die Einhaltung der Datenschutzgesetze hin
Stellv. Datenschutz-beauftragter	Name und Kontakt	
Interner Datenschutz-Koordinator	Name, Kontakt Evtl. Name, Kontakt weiterer interner Koordinatoren vor Ort in Niederlassungen, (Tochter-) Gesellschaften	-erster Ansprechpartner des DSB -streut Informationen des DSB innerhalb des Unternehmens -beschafft Unternehmensinformationen für den DSB -stellt die direkte Verbindung zwischen DSB und Verantwortlichen her
IT-Verantwortung	Name, Kontakt	
Personal-verantwortung	Name, Kontakt	
Sonstige		

III. Datenschutz-Management

Das Datenschutz-Management der Firma XY GmbH orientiert sich an einem 21-Punkte-Plan, der vom Datenschutzbeauftragten ausgearbeitet und erstellt wurde und umfasst insbesondere die Organisation, Umsetzung und permanente Kontrolle der folgenden Themen:	
Datenschutzbeauftragter und Datenschutz-Team	• Bestellung eines (ext.) Datenschutzbeauftragten (DSB) sowie eines Stellvertreters, schriftlich festgehalten in einer Benennungsurkunde (und einem Beratungsvertrag bei Externem DSB) • Bildung eines Datenschutz-Teams, bzw. Festlegung von Verantwortlichkeiten zum Datenschutz und zur Umsetzung der hier aufgezählten Themen sowie Festlegung von Verantwortlichkeiten und Kommunikationsketten zu Datenschutzthemen • Formelle Meldung des Datenschutzbeauftragten und seines Stellvertreters bei der zuständigen Landesdatenschutzbehörde, dokumentiert durch Meldebescheinigung der Behörde • Veröffentlichung des Datenschutzbeauftragten inkl. Kontaktmöglichkeiten auf der Webseite des Verantwortlichen • Bekanntgabe des Datenschutzbeauftragten sowie des Datenschutz-Teams inkl. Kontaktmöglichkeiten bei den Mitarbeitern
Auditierung	• Initialaudit durch den ext. DSB nach Benennung • Fortan regelmäßiger Informationsaustausch innerhalb des Datenschutz-Teams sowie fachverantwortlicher Mitarbeiter zu datenschutzrelevanten Themen, Prozessänderungen, neuen Prozessen usw. • Vor Ort Audits können zudem nach Bedarf oder zu Kontrollzwecken durchgeführt werden
Maßnahmenplan	• Zur Umsetzung der durch die DSGVO und das BDSG erforderlichen Maßnahmen wurde ein Maßnahmenplan erarbeitet, um eine sukzessive Umsetzung zu gewährleisten. • Maßnahmenpläne werden zudem immer dann erarbeitet werden, wenn umfangreichere oder langfristigere Maßnahmen oder Änderungen der bestehenden und bereits ergriffenen Maßnahmen notwendig erscheinen und sich aufgrund der Wichtigkeit eine Dokumentation empfiehlt.
Schulung	• Mitarbeiterschulungen werden jährlich durchgeführt. Die Teilnahme wird dokumentiert, aus der die Teilnehmerquote hervorgeht. • Nach Bedarf werden ergänzend fach- bzw. themenspezifische Live-Workshops eingerichtet, um entweder spezielle Datenschutzthemen oder Mitarbeiter bestimmter Fachbereiche zielgerichtet zu sensibilisieren. • Mitarbeiter, deren Tätigkeit nicht als „PC-Arbeitsplatz“ zu bezeichnen ist, werden mittels Schulungs-Broschüre zum allgemeinen Datenschutz und Umgang mit personenbezogenen Daten sensibilisiert. Um die Verbindlichkeit zu unterstreichen, werden die Schulungs-Broschüren gegen Unterzeichnung einer Empfangsbestätigung verteilt.
Personaldatenschutz	• Vertraulichkeitsverpflichtungen • Einwilligungserklärungen, insb. Für die Verwendung von Mitarbeiterfotos • Mitarbeiterinformation bzgl. Der Verarbeitung von Personaldatenschutz
Informationspflichten und Betroffenenrechte	• Wahrung der Betroffenenrechte durch im Unternehmen kommunizierte Prozesse (siehe weiter unten) und schriftlich geregelte Verantwortlichkeiten zur schnellstmöglichen Bearbeitung • Dokumentation von geltend gemachten Betroffenenrechten durch den Datenschutzkoordinator • Informationspflichten gegenüber Kunden, Lieferanten und Dienstleistern

	• Informationspflichten gegenüber Bewerber • Informationspflichten gegenüber Mitarbeitern • Informationspflichten gegenüber Webseitenbesuchern
Datenschutz-Handbuch und Datenschutz-Leitlinie	• Bekenntnis der Geschäftsleitung zur Einhaltung der geltenden Datenschutzgesetze und der Datenschutzgrundsätze bei der Verarbeitung personenbezogener Daten im Rahmen eines Datenschutz-Handbuchs • Schriftliche Regelung zum konkreten und transparenten Umgang unternehmensspezifischer und datenschutzrelevanter Prozesse im Rahmen einer Datenschutz-Leitlinie • Bei Bedarf werden Arbeitsanweisungen oder Richtlinien zu Speialthemen erarbeitet, die den konkreten Umgang mit einzelnen Datenverarbeitungsanlagen, Systemen, Tool oder Prozessen regeln
Auftragsverarbeitung	• Übersicht der externen Dienstleister mit (potentiellem) Zugriff auf personenbezogene Daten • Schließung von Auftragsverarbeitungsverträgen oder adäquaten Vereinbarungen mit externen Dienstleistern mit (potentiellem) Zugriff auf personenbezogene Daten • Sofern eigene Tätigkeiten als Auftragsverarbeiter bestehen, Schließung von Auftragsverarbeitungsverträgen mit Auftraggebern • Sofern Drittstaatenübermittlung, Schließung von Standard Contractual Clauses (SCC) und Prüfung, ob ausreichende Sicherheitsgarantien vorliegen • Sofern gemeinschaftliche Verantwortung vorliegt, Schließung von Joint Controllership-Verträgen
Datensicherheitskonzept	• Erstellung und Pflege des internen Datensicherheitskonzeptes im Sinne der technisch-organisatorischen Maßnahmen unter Mithilfe des IT-Verantwortlichen
Verzeichnis von Verarbeitungstätigkeiten	• Initiale Erstellung des Verzeichnisses von Verarbeitungstätigkeiten • Kontinuierliche Pflege durch den Datenschutz-Koordinator in Absprache mit dem Datenschutzbeauftragten
Videoüberwachung (sofern vorhanden)	• Dokumentation der Videoüberwachungsanlage(n) • Durchführung der Datenschutz-Folgeabschätzung unter Einbeziehung des Datenschutzbeauftragten • Hinreichende Hinweisbeschilderung • Leichter Zugang zu Datenschutzinformationen bzgl. Der Verarbeitung personenbezogener Daten durch die Videoüberwachungsanlage(n) • Bewusstsein der Unternehmensleitung, dass bei Neuinstallation oder Änderung der Videoüberwachungsanlage(n) das Datenschutz-Team vorab zu informieren ist
Datenschutz-Folgeabschätzung	• Bewusstsein der Geschäftsleitung sowie mindestens fachverantwortlicher Mitarbeiter, wann eine Datenschutz-Folgeabschätzung erforderlich ist • Durchführung stets durch das Datenschutz-Team unter Hinzuziehung des Datenschutzbeauftragten
Marketing und Werbung	• DSGVO konforme Werbeeinwilligungen • Newsletter-Versandt an Empfänger mit dokumentierter Einwilligung oder gemäß berechtigtem Interesse • Bewusstsein der Mitarbeiter, bei Marketingmaßnahmen mit Datenschutzrelevanz das Datenschutz-Team zuvor einzubeziehen
Webseite	• DSGVO konforme Datenschutzerklärung • DSGVO konformes Kontaktformular • Webseitenverschlüsselung

	• Veröffentlichung des Datenschutzbeauftragten inkl. Kontaktdaten auf der Website
Unternehmens- / Branchenspezifische Datenschutzanforderungen	• Beachtung spezifischer Datenschutzmaßnahmen, die sich aus den Unternehmenstätigkeiten des Verantwortlichen und/oder aus branchenüblichen Risken ergeben
Datenschutzbericht	• Regelmäßige Erstellung eines Datenschutzberichts zur Vorlage bei der Geschäftsleitung zur Einschätzung des Sachstandes sowie zur Dokumentation der Rechenschaftspflichten
Notfallplan	• Erstellung eines Notfallplans durch IT-Verantwortlichen
Rollen- und Berechtigungskonzept	• Zugriffsberechtigungen zu Datenverarbeitungssystemen sind im Verzeichnis der Verarbeitungstätigkeiten enthalten • Dezidiertes Rollenkonzept kann über den IT-Verantwortlichen abgerufen werden
Löschkonzept	• Fachverantwortlichen Mitarbeitern sind die jeweils für ihren Fachbereich relevanten Aufbewahrungsfristen bekannt • Eine umfangreiche Aufstellung von Aufbewahrungsfristen liegt dem Datenschutz-Koordinator vor • Regelungen zur fachgerechten Vernichtung von papiergebundenen Daten und elektronischen Datenträgern enthält die Datenschutz-Leitlinie
Kontrolle und Überwachung	• Gewährleistung im Beratungsvertrag, dass der Datenschutzbeauftragte jederzeit die Möglichkeit und sämtliche Zugänge und Zugriffe zur Durchführung auch unangekündigter Kontrollen erhält • Dokumentation von Kontrollmaßnahmen und zusammenfassende Wiedergabe in Datenschutzberichten

IV. Wahrung von Betroffenenrechten (Kommunikationsketten)		
Betroffener macht Rechte geltend	Auskunft über verarbeitete Daten	**1.**Betroffener wendet sich über allgemeine Kontaktkanäle an den Verantwortlichen oder über datenschutz@... direkt an den Koordinator **2.**Koordinator identifiziert Anfragenden als Betroffenen und spricht mit DSB ab, ob Anfrage rechtens ist, in welchem Umfang ihr nachzugehen ist und beantwortet diese
	Berichtigung von Daten	**1.**Betroffener wendet sich über allgemeine Kontaktkanäle an den Verantwortlichen oder über datenschutz@... direkt an den Koordinator **2.**Koordinator gibt Info zur Datenänderung an jeweiligen Fachverantwortlichen und/oder Systemverantwortlichen weiter, damit die Datenänderung in den relevanten Systemen übernommen wird
	Löschen / Sperren von Daten	**1.**Betroffener wendet sich über allgemeine Kontaktkanäle an den Verantwortlichen oder über datenschutz@... direkt an den Koordinator **2.**Koordinator erörtert mit DSB, ob Anspruch auf Löschung/Sperrung besteht und informiert Betroffenen über das Ergebnis und das weitere Vorgehen **a)**Positiv-Antwort: Dem Begehren wird nachgekommen; Info an Fachverantwortliche oder

		Systemverantwortliche, dass Daten gelöscht/gesperrt werden sollen **b)**Negativ-Antwort: Betroffener erhält Info, dass und aus welchen Gründen nicht gelöscht/gesperrt werden darf
	Widerruf von Einwilligungen	**1.**Betroffener wendet sich über allgemeine Kontaktkanäle an den Verantwortlichen oder über datenschutz@... direkt an den Koordinator **2.**Koordinator gibt unverzüglich Info an Fachverantwortliche und Systemverantwortliche, dass und welche Daten vom Widerruf umfasst sind und dass die konkrete Datenverarbeitung unverzüglich einzustellen ist **3.**Info an Betroffenen, dass Widerspruch eingegangen ist und dem nachgekommen wird
	Information bzgl. Datenpanne	**1.**Datenpanne ist eingetreten **2.**Koordinator und DSB werden unverzüglich von Geschäftsführung oder Fachverantwortlichen informiert und werten weitere Schritte aus. **3.**Weitere Schritte können u.U. sein ●Information des Betroffenen ●Meldung an die Behörde **4.**Koordinator und DSB regen ggü. Fachverantwortlichen, Systemverantwortlichen und u.U. Geschäftsführung an, Maßnahmen zu ergreifen, um künftige Datenpannen der Art zu vermeiden und Sicherheitslücken zu schließen
Auskunfts-ersuchen von Dritten	Dritter erbittet Auskunft zu personenbezogenen Daten (z.B. Behörde, Kreditinstitut, Auskunftei o.Ä.)	**1.**Auskunftsersuchender wendet sich über allgemeine Kontaktkanäle an den Verantwortlichen, an einen Mitarbeiter oder über datenschutz@... direkt an den Koordinator **2.**Koordinator und DSB prüfen, ob Auskunft gewährt werden darf. **a)**Positiv-Antwort: Auskunft wird gewährt (und dokumentiert) **b)**Negativ-Antwort: Auskunft wird verweigert und die Verweigerung begründet (und dokumentiert)
Datenschutz-aufsichtsbehörde sucht Kontakt zum Verantwortlichen oder DSB	Vielfältige Gründe für Kontaktaufnahme der Behörde denkbar, z.B. aufgrund von Beschwerde, stichprobenartige/anlasslose oder anlassbezogene Überprüfung	**1.**Behörde wendet sich i.d.R. direkt an Kontakt des DSB oder an Geschäftsführung **2.**Anfrage wird von DSB, u.U. nach interner Erörterung der Sachlage bearbeitet und dokumentiert
Datenschutz-panne im Unternehmen eingetreten	Datenschutzpanne kann u.U. bereits vorliegen beim Verlust eines Diensthandys, Laptops oder USB-Sticks, bei Herausgabe von personenbezogenen Daten an unberechtigte Empfänger oder bei Datenverlust durch (unachtsame) Handlungen von Mitarbeitern (z.B. Datenlöschung im System)	**1.**Nach Kenntniserlangung der (vermuteten) Datenpanne werden Koordinator und DSB unverzüglich informiert. **2.**Koordinator und DSB erörtern (u.U. gemeinsam mit Fachverantwortlichen, Systemverantwortlichen und Geschäftsführung) mögliche Folgen für etwaige Betroffene **3.**Abhängig vom Ergebnis der Erörterung sind u.U. Maßnahmen zu treffen

		●Information des Betroffenen ●Meldung an die zuständige Behörde ●Schließen des Lecks und Ausbessern von technisch-organisatorischen Maßnahmen zur Vermeidung weiterer Pannen
Notfall	Gemeint sind insbesondere (schwere) Notfälle, wie z.B. Ausfall des Rechenzentrums, Verlust/Zerstörung von personenbezogenen Daten aufgrund von Brand- oder Wasserschäden im Gebäude, Einbruch o.Ä.	**1.**Nach Kenntniserlangung werden Koordinator und DSB unverzüglich informiert. **2.**Koordinator und DSB erörtern (u.U. gemeinsam mit Fachverantwortlichen, Systemverantwortlichen und Geschäftsführung) mögliche Folgen für etwaige Betroffene **3.**Abhängig vom Ergebnis der Erörterung sind u.U. Maßnahmen zu treffen ●Information des Betroffenen ●Meldung an die zuständige Behörde ●Koordinator und DSB regen ggü. Fachverantwortlichen, Systemverantwortlichen und u.U. Geschäftsführung an, Maßnahmen zu ergreifen, um künftige Datenpannen der Art zu vermeiden und Sicherheitslücken zu schließen

V. Aufgabenwahrnehmung & Dokumentation	
Berichte & Maßnahmen-pläne	●Werden zentral und chronologisch vom Koordinator aufbewahrt zur Gewährleistung der Rechenschaftspflicht ●Berichte werden an Geschäftsleitung weitergeleitet ●Sofern unternehmenspolitische Entscheidungen zu treffen sind, die sich aus Maßnahmenplan und/oder Bericht ergeben, zeitnahe Absprache mit Geschäftsführung
Geltendmachung von Betroffenen-rechten	●Wesentliche Kommunikation (insb. Mit Betroffenem) wird zentral und jederzeit auffindbar vom Koordinator aufbewahrt ●Interne Anweisungen betreffend der Geltendmachung (z.B. Aufforderung zum Löschen von Daten) werden zentral jederzeit auffindbar vom Koordinator aufbewahrt ●Im Falle eines positiven Löschanspruchs wird dies dokumentiert und zentral und jederzeit auffindbar vom Koordinator aufbewahrt ●Unverzügliche Einbeziehung des DSB
Behörden-kommunikation	●Findet i.d.R. direkt mit dem DSB statt, der die Kommunikation dokumentiert und zentral aufbewahrt ●Koordinator sollte Kommunikation zusätzlich zentral und jederzeit auffindbar aufbewahren
Auftrags-verarbeitung	●Mitarbeiter, die eigenständig über die Beauftragung von externen Dienstleistern entscheiden dürfen, sind darüber informiert, dass mit Dienstleistern ein Auftragsverarbeitungsvertrag oder eine Vertraulichkeitsvereinbarung zu schließen ist, sofern ein Zugriff des Dienstleisters auf personenbezogene Daten nicht ausgeschlossen werden kann. ●Die entsprechenden Mitarbeiter informieren in diesen Fällen vor Beauftragung den Koordinator oder den DSB. ●Eingehende Auftragsverarbeitungsverträge und Vertraulichkeitsvereinbarungen sind vor Unterzeichnung zur Prüfung an den Koordinator oder den DSB zu übersenden. ●Gezeichnete Auftragsverarbeitungsverträge und Vertraulichkeitsvereinbarungen sind vom Koordinator zentral und jederzeit auffindbar aufzubewahren.

***Hinweise zur Verwendung**

Bei dem vorliegenden Dokument handelt es sich um ein kostenloses Muster, das keinen Anspruch auf Vollständigkeit und Richtigkeit erhebt. Die Vorlage sollte stets auf die individuellen Bedürfnisse und die Umstände des Einzelfalls angepasst und ggf. fachkundig geprüft werden.

Die Vorlage darf für eigene Zwecke oder Zwecke Ihres Unternehmens verwendet werden. Die Weitergabe an Dritte, z.B. an eigene Kunden, sowie die kommerzielle Nutzung sind ohne ausdrückliche Genehmigung nicht gestattet.

exkulpa gmbh
Waldfeuchter Str. 266 / 52525 Heinsberg
Tel: 02452 / 99 33 11 @: info@exkulpa.de
www.exkulpa.de