Datenschutzrichtlinie

Experts in perimeterprotection

Datenschutzrichtlinie

1. Regelungszweck

1.1. In dieser Richtlinie wird beschrieben, wie Heras („das Unternehmen",) personenbezogene Daten von Beschäftigten oder Geschäftspartnern verarbeitet.

1.2. Personenbezogene Daten werden gemäß der Datenschutz-Grundverordnung (Verordnung (EU) 2016/679) und anderer anwendbarer nationaler Datenschutzgesetzte wie z.B. das Bundesdatenschutzgesetz (gemeinsam das „Datenschutzgesetz") verarbeitet.

1.3. In dieser Datenschutzrichtlinie kursiv markierte Begriffe werden im Glossar in Anhang I definiert.

1.4. Des Weiteren beschreiben wir,

1.4.1. welche Rechte und Wahlmöglichkeiten Personen im Zusammenhang mit unserer Nutzung ihrer personenbezogenen Daten haben.

1.4.2. die Maßnahmen, die wir ergreifen, um die Datensicherheit zu gewährleisten, und wie Sie uns zu Fragen über unsere Datenschutzpraktiken und zur Ausübung Ihrer Rechte kontaktieren können.

1.5. Für die Heras Deutschland GmbH gibt es zum Datenschutz eine Betriebsvereinbarung zur „Einführung und Nutzung von IT-Systemen sowie zur Verarbeitung von Beschäftigtendaten", derzeit in der Fassung vom 21.06.2023. Die jeweils gültigen gesetzlichen Regelungen nach deutschem Recht sowie die Betriebsvereinbarungen in ihrer jeweils aktuell geltenden Fassung gehen dieser allgemeinen Datenschutzrichtlinie jederzeit vor.

2. Geltungsbereich

2.1. Diese Datenschutzrichtlinie gilt für das Unternehmen.

2.2. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten.

2.3. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

2.4. Sofern in anderen Unternehmen der Heras Unternehmensgruppe personenbezogene Daten der Beschäftigten des Unternehmens verarbeitet werden, so wird diese Richtlinie darauf ebenfalls angewendet.

3. Prinzipien für die Verarbeitung personenbezogener Daten

3.1. Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Beschäftigten gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise erhoben und verarbeitet werden.

3.2. Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen der Zustimmung durch den Betriebsrat und der Beschäftigten.

3.3. Markt- und Meinungsforschung

Die Verarbeitung personenbezogener Daten zum Zwecke der Markt- und Meinungsforschung ist untersagt.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

3.4. Transparenz

Der Beschäftigte muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Beschäftigten selbst zu erheben. Bei Erhebung der Daten muss der Beschäftigte mindestens Folgendes erkennen können oder entsprechend informiert werden über:

3.4.1. Die Identität der verantwortlichen Stelle

3.4.2. Den Zweck der Datenverarbeitung

3.4.3. Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

3.5. Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben.

3.6. Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

3.7. Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

3.8. Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

4. Zulässigkeit der Datenverarbeitung

4.1. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der Erlaubnistatbestände gemäß Ziffer 5. Mitarbeiterdaten/Bewerberdaten vorliegt.

4.2. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

5. Mitarbeiterdaten/Bewerberdaten

5.1. In der o.g. Betriebsvereinbarung ist aufgelistet, welche personenbezogenen Daten zu welchem Zweck verarbeitet werden.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

5.2. Neben den in der Betriebsvereinbarung dargelegten Kategorien personenbezogener Daten verarbeitet das Unternehmen außerdem die folgenden Kategorien an personenbezogenen Daten:
  5.2.1. Daten in Bezug auf das Führen von Leasingfahrzeugen auf das amtliche Kennzeichen eines Leasingfahrzeugs
5.3. Neben den in 5.1 und 5.2 dargelegten Daten und Zwecken verarbeitet das Unternehmen personenbezogene Daten für keine zusätzliche Zwecke.
5.4. Das Unternehmen führt kein Profiling durch.
5.5. Datenverarbeitung
  5.5.1. Datenverarbeitung für das Arbeitsverhältnis
    5.5.1.1. Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind.
    5.5.1.2. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.
    5.5.1.3. Ist im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen erforderlich, sind die jeweiligen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betriebsrats und des Beschäftigten einzuholen.
    5.5.1.4. Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit dem Betriebsrat, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.
  5.5.2. Aufgrund gesetzlicher Erlaubnis
    5.5.2.1. Die Verarbeitung personenbezogener Mitarbeiterdaten ist zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten.
    5.5.2.2. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.
    5.5.2.3. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden. Siehe § 147 AO, § 257 HGB, § 107 GewO.
  5.5.3. Kollektivregelungen für Datenverarbeitungen
    5.5.3.1. Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird.
    5.5.3.2. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Betriebsrat im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts.
    5.5.3.3. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.
  5.5.4. Aufgrund von berechtigtem Interesse
    5.5.4.1. Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des Unternehmens erforderlich ist.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

5.5.4.2. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) begründet.
5.5.4.3. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen.
5.5.4.4. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.
5.5.4.5. Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist.
5.5.4.6. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden.
5.5.4.7. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind.
5.5.4.8. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden.
5.5.4.9. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte des Betriebsrats und Informationsrechte der Beschäftigten) berücksichtigt werden.

5.5.5. Besonders schutzwürdige Daten

5.5.5.1. Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.
5.5.5.2. Besonders schutzwürdige Daten sind Daten über
5.5.5.2.1. die rassische und ethnische Herkunft,
5.5.5.2.2. über politische Meinungen
5.5.5.2.3. religiöse oder philosophische Überzeugungen
5.5.5.2.4. Gewerkschaftszugehörigkeiten
5.5.5.2.5. die Gesundheit
5.5.5.2.6. Sexualleben des Beschäftigten
5.5.5.3. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.
5.5.5.4. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.
5.5.5.5. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein.
5.5.5.6. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann.
5.5.5.7. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen.
5.5.5.8. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

5.5.5.9. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte des Betriebsrats und Informationsrechte der Beschäftigten) berücksichtigt werden.

5.5.6. Datenübermittlung

5.5.6.1. Das Unternehmen legt personenbezogene Daten ausschließlich zu den in der Betriebsvereinbarung genannten Zwecken offen oder stellt sie diesen bereit.

5.5.6.2. Im Rahmen der regulären Geschäftstätigkeit des Unternehmens werden personenbezogene Daten gemäß o.g. Betriebsvereinbarung an Auftragsverarbeiter weitergeleitet.

5.5.6.3. Der Empfänger der Daten ist im Vorfeld darauf verpflichtet worden, diese nur zu den festgelegten Zwecken zu verwenden und sie gegebenenfalls nach Aufforderung durch das Unternehmen zu löschen.

5.5.6.4. Vor der Übermittlung der Daten sind die Standards unter Ziffer 3 einzuhalten.

5.5.7. Datenspeicherung

5.5.7.1. Bei Umsetzung einer Datenlöschung oder eines Auskunftsersuchen muss der Datenschutzbeauftragte dem vollumfänglich nachkommen können.

5.5.8. Auskunftsrecht

5.5.8.1. Jeder Mitarbeiter hat das Recht umfänglich über seine, beim Unternehmen gespeicherten personenbezogenen Daten Auskunft zu erhalten. Die Einsicht in die Daten beantragen Sie unter folgender E-Mail-Adresse: siehe Anhang II „Datenschutzbeauftragter“

5.5.9. Datenlöschung

5.5.9.1. Das Löschkonzept ist als Anlage zur o.g. Betriebsvereinbarung definiert.

5.5.9.2. Nach § 257 Abs. 1 Nr. 1 und 4 HGB sind Personalakten sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen zehn Jahre aufzubewahren.

5.5.9.3. Nach der 10-Jahres-Frist werden die personenbezogenen Daten gelöscht, oder soweit anonymisiert, dass eine Rückverfolgung nicht oder nur unter Einsatz eines enormen Aufwandes durchgeführt werden kann.

6. Auftragnehmer- und Kundendaten

6.1. Das Unternehmen erhebt und verarbeitet personenbezogene Daten in Bezug auf Personen, die Lieferanten und Kunden sind und/oder mit diesen zusammenarbeiten.

6.2. Zu diesen personenbezogenen Daten können gehören:

6.2.1. Persönliche Angaben wie Name, Titel, Position, Abteilung, Geschäftsbereich

6.2.2. sowie Kontaktangaben wie E-Mailadresse, Telefonnummer(n) und Arbeitsort

6.2.3. darüber hinaus steuerliche Angaben wie Umsatzsteuer-Identifikationsnummern und Steuernummern.

6.2.4. Es gelten für Lieferanten und Kundendaten ebenfalls die Regelungen in Ziffer 5.5.2. - 5.5.9

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

7. Telekommunikation und Internet

7.1. Telefonanlagen, E-Mailadressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource.

7.2. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden.

7.3. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden.

7.4. Eine generelle Überwachung der Telefon- und E-Mailkommunikation bzw. der Intranet- und Internetnutzung findet nicht statt.

7.5. Zur Abwehr von Angriffen auf die IT¬Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das Heras¬-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren.

7.6. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mailadressen, des Intranets und Internets sowie der internen sozialen Netzwerke nach Genehmigung durch den Betriebsrat zeitlich befristet protokolliert werden.

7.7. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens erfolgen.

7.8. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen.

8. Auftragsdatenverarbeitung

8.1. Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird.

8.2. In diesen Fällen ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb der Heras Unternehmensgruppe eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen.

8.3. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung.

8.4. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

8.5. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten. Der beauftragende Fachbereich muss ihre Umsetzung sicherstellen:

8.5.1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

8.5.2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

8.5.3. Die vom Datenschutzbeauftragten bereitgestellten Vertragsstandards müssen beachtet werden.

8.5.4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen.

8.5.5. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

8.5.6. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen.

8.5.7. Insbesondere darf die Verarbeitung personenbezogener Daten nur im Europäischen Wirtschaftsraum stattfinden.

9. Rechte des Beschäftigten

9.1. Jeder Beschäftigte kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Beschäftigten zu keinerlei Nachteilen führen.

9.1.1. Der Beschäftigte kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

9.1.2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

9.1.3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Beschäftigte ihre Berichtigung oder Ergänzung verlangen.

9.1.4. Der Beschäftigte ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist.

9.1.5. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist.

9.1.6. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

9.1.7. Der Beschäftigte hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten.

9.1.8. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

9.1.9. Darüber hinaus kann jeder Beschäftigte die in der Datenschutzrichtlinie eingeräumten Rechte als Drittbegünstigter geltend machen, wenn ein Unternehmen, das sich zur Einhaltung der Datenschutzrichtlinie verpflichtet hat, deren Vorgaben nicht beachtet und er dadurch in seinen Rechten verletzt ist.

9.1.10. Beantwortung eines Antrags

9.1.10.1. Ein Antrag muss an den Datenschutzbeauftragten des Unternehmens gestellt werden. Das Unternehmen ist gehalten, die antragstellende Person sowie alle dritten Parteien, denen die personenbezogenen Daten übermittelt worden sind, über Änderungen, Löschungen oder Einschränkungen nach deren Durchführung zu informieren.

9.1.10.2. Als Reaktion auf einen Antrag übermittelte Informationen oder Kommunikationen für oder mit einer Person müssen:

9.1.10.2.1. in einem knappen, deutlichen, leicht verständlichen und einfach zugänglichen Format unter Verwendung einer klaren Sprache abgefasst sein;

9.1.10.2.2. schriftlich stattfinden (z. B. per Brief oder E-Mail); und

9.1.10.2.3. wurde ein Antrag von einer Person in elektronischer Form gestellt (z. B. per E-Mail), ist die Antwort, wenn möglich, ebenfalls in elektronischer Form abzufassen (d. h. per E-Mail), vorbehaltlich anderslautender Anweisungen der Person.

9.1.11. Frist zur Beantwortung eines Antrags

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

9.1.11.1. Nach Eingang eines gültigen Antrags hat die Antwort „ohne unangemessene Verzögerung", in jedem Fall jedoch spätestens einen Monat nach Erhalt des Antrags zu erfolgen.

9.1.11.2. Diese Frist von einem Monat kann bei Bedarf um zwei weitere Monate verlängert werden, unter Berücksichtigung der Komplexität und Anzahl der eingehenden Anträge.

9.1.11.3. Das Unternehmen hat die Person über jede solcher Verlängerungen innerhalb des ersten Monats des Antragseingangs zu informieren, einschließlich der Gründe für die Verzögerung/ Verlängerung.

9.1.11.4. Liegen dem Unternehmen gültige und legitime Gründe für eine Nichtbeantwortung eines Antrags innerhalb des vorgegebenen Zeitrahmens vor, ist sie gehalten:

9.1.11.4.1. die Person „unverzüglich", spätestens jedoch innerhalb eines Monats nach Eingang des Antrags über die Gründe der ausbleibenden Bearbeitung in Kenntnis zu setzen

9.1.11.4.2. die Person über sein/ihr Recht zur Einreichung einer Beschwerde bei der zuständigen Datenschutzbehörde zu informieren

9.1.12. Kosten für die Beantwortung eines Antrags

9.1.13. Alle Informationen/Kommunikationen seitens des Unternehmens im Zusammenhang mit einem Antrag sind kostenfrei zu erbringen.

10. Vertraulichkeit der Verarbeitung

10.1. Personenbezogene Daten unterliegen dem Datengeheimnis.

10.2. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist allen, für das Unternehmen tätigen Personen, untersagt. Dies umfasst alle Hierarchiestufen einschließlich der Geschäftsleitung.

10.3. Unbefugt ist jede Verarbeitung, die eine Person vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein.

10.4. Es gilt das Need-to¬know-Prinzip: alle Personen dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist.

10.5. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

10.6. Alle Personen dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen.

10.7. Alle Personen müssen bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichtet werden.

10.8. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

11. Sicherheit der Verarbeitung

11.1. Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

11.2. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.
11.3. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen.
11.4. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren.
11.5. Der verantwortliche Fachbereich muss dazu insbesondere den Datenschutzbeauftragten zu Rate ziehen.
11.6. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des Heras-weiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

12. Datenschutzkontrolle

12.1. Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft.
12.2. Die Durchführung obliegt dem Datenschutzbeauftragten oder beauftragten externen Prüfern.
12.3. Die Geschäftsführer des Unternehmens sind im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren.
12.4. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt.
12.5. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

13. Datenschutzvorfälle

13.1. Jeder Beschäftigte muss die Geschäftsführung oder dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) melden.
13.2. Die Geschäftsführung ist verpflichtet, den Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten.
13.3. In Fällen von unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder bei Verlust personenbezogener Daten sind die im Unternehmen vorgesehenen Meldungen unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.
13.4. Verfahren bei Verletzung des Schutzes personenbezogener Daten
13.4.1. Einführung

Vorliegendes Verfahren bei Verletzung des Schutzes personenbezogener Daten (das „Verfahren") beschreibt den Prozess der Eskalation, Meldung und Aufzeichnung vermuteter oder tatsächlicher Verletzungen des Schutzes personenbezogener Daten (gemäß nachstehender Definition). Dieses Verfahren gilt für Heras (das „Unternehmen"). Der Zweck dieses Verfahrens besteht darin, sicherzustellen, dass das Unternehmen sämtliche Verletzungen des Schutzes personenbezogener Daten (wie nachstehend definiert) unverzüglich bearbeitet und begrenzt, damit die Auswirkungen der Datenschutzverletzung minimiert und alle rechtlichen Verpflichtungen zur Meldung von Datenschutzverletzungen an eine Regulierungsbehörde und/oder eine oder mehrere durch die Datenschutzverletzung betroffenen

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

Person(en) (in Übereinstimmung mit der Datenschutzgrundverordnung (Verordnung (EU) 2016/679) sowie dem Bundesdatenschutzgesetz) fristgerecht erfüllt werden können.

13.4.2. Was ist eine Verletzung des Schutzes personenbezogener Daten?

13.4.2.1. Die Datenschutzgrundverordnung definiert eine Verletzung des Schutzes personenbezogener Daten als „eine Verletzung der Sicherheit, die eine versehentliche oder rechtswidrige Vernichtung, den Verlust, die Änderung, eine unerlaubte Offenlegung von oder den Zugriff auf übertragene, gespeicherte oder in anderer Weise verarbeitete Daten zur Folge hat („Verletzung des Schutzes personenbezogener Daten“).

13.4.2.2. Eine Verletzung des Schutzes personenbezogener Daten ist jede unberechtigte oder versehentliche Offenlegung, jeder Verlust oder jegliche sonstige Form der unberechtigten, versehentlichen oder ungesetzmäßigen Erhebung, Nutzung, Aufzeichnung, Speicherung oder Verbreitung personenbezogener Daten. Beispiele für Verletzungen des Schutzes personenbezogener Daten sind: Verlust oder Diebstahl eines Laptops oder Mobiltelefons, auf denen personenbezogene Daten gespeichert sind; Versand einer (ungeschützten) Excel-Datei mit personenbezogenen Daten an eine unberechtigte Person; das Drucken von Lohnangaben und das anschließende Zurücklassen der Papiere auf einem Drucker; Hacken eines Systems, auf dem personenbezogene Daten gespeichert sind; und/oder Verlust oder Diebstahl von Dateien usw.

13.4.2.3. Ein Vorfall mit einer Verletzung der Datensicherheit wird als „Datenleck” bezeichnet.

13.4.2.4. Sind bei einem Datenleck keine personenbezogenen Daten involviert, handelt es sich nicht um eine Verletzung des Schutzes personenbezogener Daten.

13.4.2.5. Darüber hinaus sind nicht alle Datenlecks, bei denen personenbezogene Daten betroffen sind, Verletzungen des Schutzes personenbezogener Daten. So kann beispielsweise der Verlust oder die Beeinträchtigung von personenbezogenen Daten nicht als Verletzung des Schutzes personenbezogener Daten gelten, wenn:

13.4.2.5.1. die personenbezogenen Daten verschlüsselt oder anonymisiert sind;

13.4.2.5.2. im Falle eines Datenverlustes ein vollständiges, aktuelles Backup der personenbezogenen Daten existiert;

13.4.2.5.3. der Zugriff auf die personenbezogenen Daten überwacht wird.

13.4.2.6. Demnach ist die Entscheidung, ob ein Datenleck eine Verletzung des Schutzes personenbezogener Daten darstellt, fallweise zu treffen.

13.4.3. Wann kommt dieses Verfahren zur Anwendung?

13.4.3.1. Sind bei einem Datenleck keine personenbezogenen Daten betroffen, kommt dieses Verfahren nicht zur Anwendung.

13.4.3.2. Sind bei einem Datenleck jedoch personenbezogene Daten betroffen, kann eine Verletzung des Schutzes personenbezogener Daten vorliegen und dieses Verfahren kommt zur Anwendung.

13.4.3.3. Bestehen Zweifel darüber, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt, sollte sich das Unternehmen zwecks Beratung unverzüglich an den Geschäftsführer wenden, um die Situation schnellstmöglich zu prüfen.

13.4.4. Wie melde ich intern eine Verletzung des Schutzes personenbezogener Daten?

Es ist zu beachten, dass alle aktuellen oder vermuteten Verletzungen des Schutzes personenbezogener Daten unverzüglich intern bei Heras gemäß folgender Schritte gemeldet werden müssen:

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

13.4.4.1. Erstmeldung

13.4.4.1.1. Wurde eine tatsächliche oder vermutete Verletzung des Schutzes personenbezogener Daten wahrgenommen, ist dies unverzüglich der Geschäftsführung oder dem Datenschutzbeauftragten der Gruppe zu melden.

13.4.4.2. Reaktionsplanung: folgende Maßnahmen müssen ergriffen werden:

13.4.4.2.1. Zusammenstellung von Informationen über die Meldung über die Verletzung des Schutzes personenbezogener Daten

13.4.4.2.2. Festlegung von Maßnahmen zur unverzüglichen Eindämmung der Verletzung des Schutzes personenbezogener Daten

13.4.4.2.3. Überprüfung, ob ein Erfordernis besteht, die zuständige Datenschutzbehörde („DSB") über die Verletzung des Schutzes personenbezogener Daten zu informieren und wenn ja, was gemeldet werden muss;

13.4.4.2.4. Bestimmung der sich aus der Verletzung des Schutzes personenbezogener Daten für das Unternehmen und die Beschäftigten Personen ableitenden Konsequenzen; die Maßnahmen, die das Unternehmen zu diesem Zeitpunkt ergreift und/oder ergreifen kann, um den Schaden für die betroffenen Personen abzumildern;

13.4.4.2.5. Festlegung der Art und Weise, wie die betroffenen Personen über die Verletzung des Schutzes personenbezogener Daten gegebenenfalls unter den vorherrschenden Umständen zu informieren sind, sowie die Maßnahmen, die die Personen zur Minderung weiterer Schäden ergreifen können

13.4.4.2.6. Klärung, ob sich eine aus der Verletzung des Schutzes personenbezogener Daten ableitende persönliche Haftung oder eine Haftung seitens dritter Parteien ergibt;

13.4.4.2.7. Bestimmung interner (und bei Bedarf externer) Kommunikationen und deren zeitlicher Ablauf;

13.4.4.2.8. Klärung, ob neben der DSB auch andere Beteiligte zu informieren sind; und

13.4.4.2.9. Klärung, welche Lehren aus der Verletzung des Schutzes personenbezogener Daten gezogen und welche Maßnahmen ergriffen werden können, um ein Wiederauftreten zu verhindern

13.4.4.3. Meldung an die DSB notwendig?

13.4.4.3.1. Nicht jede Verletzung des Schutzes personenbezogener Daten ist der DSB zu melden. So ist es beispielsweise nicht notwendig, die DSB in Kenntnis zu setzen, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich kein Risiko für irgendwelche Personen nach sich ziehen wird.

13.4.4.3.2. Ist die Meldung einer Verletzung des Schutzes personenbezogener Daten an die entsprechende DSB notwendig, wird der Datenschutzbeauftragte diese Verletzung des Schutzes personenbezogener Daten der zuständigen DSB nach Rücksprache mit der Geschäftsführung melden.

13.4.4.3.3. Die Meldung an die zuständige DSB sollte schnellstmöglich und falls machbar spätestens innerhalb von 72 Stunden erfolgen, nachdem die Verletzung des Schutzes personenbezogener Daten zutage getreten ist.

13.4.4.3.4. Findet eine Meldung nicht innerhalb von 72 Stunden statt, ist der DSB eine stichhaltige Begründung für die Verspätung zu liefern.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

13.4.4.4. Beseitigung

13.4.4.4.1. Nach der Meldung an die zuständige DSB und unter Berücksichtigung eventueller Bemerkungen der Behörde wird sich der Datenschutzbeauftragte mit der Geschäftsführung in Bezug auf die Abwicklung und Beseitigung der Verletzung des Schutzes personenbezogener Daten gemäß dem entsprechenden Reaktionsplan „Verletzung des Schutzes personenbezogener Daten“ beraten.

13.4.5. Was ist der DSB zu melden?

Bei der Erstellung einer Meldung ist die DSB zu informieren über:

13.4.5.1. die Art der Verletzung des Schutzes personenbezogener Daten, einschließlich der Kategorien personenbezogener Daten und der betroffenen Personen, die Anzahl der betroffenen Personen sowie der Umfang der kompromittierten personenbezogenen Daten;

13.4.5.2. die voraussichtlichen, aus der Verletzung des Schutzes personenbezogener Daten zu erwartenden Konsequenzen;

13.4.5.3. die ergriffenen Maßnahmen oder vorgeschlagenen zu ergreifenden Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten;

13.4.5.4. die Maßnahmen, die von den betroffenen Personen zur Begrenzung schädlicher Folgen ergriffen werden können, die sich aus der Verletzung des Schutzes personenbezogener Daten ableiten; und

13.4.5.5. der Name und die Kontaktangaben des Ansprechpartners des Unternehmens, bei dem weitere Informationen in Bezug auf die Verletzung des Schutzes personenbezogener Daten angefordert werden können

13.5. Meldung einer Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen

13.5.1. Die betroffenen Personen ist nur dann zu informieren, wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich in einem „hohen Risiko“ für die Rechte und Freiheiten der betroffenen Personen resultieren wird.

13.5.2. Die Meldung der Verletzung des Schutzes personenbezogener Daten an die betroffenen Personen findet gemäß dem betreffenden Reaktionsplan statt.

13.5.3. Die an die betroffenen Personen zu übermittelnde Meldung hat mindestens zu enthalten:

13.5.3.1. Art und Umfang der Datenschutzverletzung

13.5.3.2. die zur Begrenzung der negativen Folgen der Verletzung des Schutzes personenbezogener Daten ergriffenen Maßnahmen

13.5.3.3. eine Beschreibung der sowohl festgestellten als auch vermuteten Folgen der Verletzung des Schutzes personenbezogener Daten für die betroffenen Personen.

13.5.3.4. die Maßnahmen, die das Unternehmen ergriffen hat oder vorschlägt zu ergreifen, um die Folgen der Verletzung des Schutzes personenbezogener Daten zu begrenzen.

13.5.4. Eine Meldung an Personen ist nicht erforderlich, wenn

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

13.5.4.1. das Unternehmen angemessene technische und organisatorische Maßnahmen ergriffen hat, durch die die personenbezogenen Daten für jede für den Zugriff unberechtigte Person nicht lesbar sind, beispielsweise die Verwendung einer Verschlüsselungstechnik

13.5.4.2. das Unternehmen im Nachgang Maßnahmen ergriffen hat, mit denen sichergestellt ist, dass das hohe Risiko für Personen wahrscheinlich nicht eintreten wird.

14. Verantwortlichkeiten und Sanktionen

14.1. Die Geschäftsführung des Unternehmens ist verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich.

14.2. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten).

14.3. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.

14.4. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Beschäftigten.

14.5. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

14.6. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Beschäftigten ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen und ist eine vorherige Zustimmung des Betriebsrats erforderlich.

14.7. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten.

14.8. Die Führungskräfte müssen sicherstellen, dass ihre Beschäftigten im erforderlichen Umfang zum Datenschutz geschult werden.

14.9. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht wird auch strafrechtlich verfolgt und kann Schadensersatzansprüche nach sich ziehen.

15. Der Datenschutzbeauftragte

15.1. Der Datenschutzbeauftragte als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der Datenschutzvorschriften hin.

15.2. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung.

15.3. Der Datenschutzbeauftragte wird von der Geschäftsführung der Heras Unternehmensgruppe bestellt.

15.4. Jeder Beschäftigte kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden.

15.5. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

15.6. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung ist durch die Geschäftsführung zu berücksichtigen.

15.7. Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten zur Kenntnis zu bringen.

15.8. Name und Kontaktdaten des Datenschutzbeauftragten sind der Anlage II zu entnehmen.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

Anhang I
GLOSSAR

In vorliegender Datenschutzrichtlinie besitzen nachfolgende Begriffe die folgende Bedeutung:

- „Anonymisiert“ sind Daten dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.

- „Verantwortliche Stelle“ ist das Unternehmen.

- Dritter ist jeder außer dem Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Auftragsdatenverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

- „Beschäftigter“ im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden.

- „Datenschutzvorfälle“ sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Beschäftigte beziehen.

- Von einer „Grenzüberschreitenden Verarbeitung“ ist die Rede, wenn: (a) wir in mehr als einem EU Mitgliedsstaat ansässig sind und die Verarbeitung von personenbezogenen Daten durch uns in mehr als einem EU-Mitgliedsstaat stattfindet; oder (b) die Verarbeitung von personenbezogenen Daten durch uns in lediglich einem EU-Mitgliedsstaat stattfindet und sich diese Verarbeitung in erheblicher Weise (oder wahrscheinlich in erheblicher Weise) auf Personen in mehr als einem EU-Mitgliedsstaat auswirkt.

- „Verletzung des Schutzes personenbezogener Daten” bezeichnet eine Verletzung der Sicherheit, die eine versehentliche oder rechtswidrige Vernichtung, den Verlust, die Änderung, eine unerlaubte Offenlegung von oder den Zugriff auf übertragene, gespeicherte oder in anderer Weise verarbeitete Daten zur Folge hat.

- „Datenverantwortlicher” bezeichnet das Rechtssubjekt, das entscheidet, warum und wie personenbezogene Daten verarbeitet werden.

- „Datenverarbeiter” bezeichnet die Partei, die personenbezogene Daten im Auftrag des Datenverantwortlichen verarbeitet (beispielsweise ein Dienstleister im Bereich Lohnbuchhaltung).

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

- „Europäischer Wirtschaftsraum" oder "EWR" umfasst die Länder Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Republik Zypern, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Liechtenstein und Ungarn.

- „Personenbezogene Daten" bezeichnet alle Informationen zu einer lebenden Person, die eine Identifikation dieser Person ermöglichen. Eine Person ist dann identifizierbar, wenn ihre Identität in angemessener Weise ohne jeglichen unverhältnismäßigen Aufwand aus den Daten abgeleitet werden kann. Zu personenbezogenen Daten können gehören:
  - Mitarbeitende
    1. Persönliche Angaben wie Name, Geburtsdatum, Kontodaten, Familienangehörige
    2. Kontaktangaben wie Adresse und Telefonnummer(n);
    3. Einzelheiten der Personalakte wie Beschäftigungsbedingungen, Ausbildung, Leistungsbeurteilungen, Beförderungen, persönliche Entwicklungspläne, verhaltensbezogene und disziplinarische Daten, Arbeitsort, Gehaltsinformationen, Kontodetails personenbezogene identifizierbare Nummern wie Steuernummern und Sozialversicherungsnummern;
    4. Beschäftigungshistorie, Daten zur Ausbildung, Bewerbungsdetails
    5. Medizinische Daten wie ärztliche Atteste und Krankschreibungen;
    6. Angaben zu Familie wie Namen und Geburtsdaten von Kindern; dies ist beispielsweise relevant, wenn eine Person Elternzeit beantragt;
    7. rentenrelevante Daten und Informationen
    8. Leistungsbezogene Daten wie Leistungs-Management-Bewertungen, z.B. in Jahresgesprächen, Entwicklungsgesprächen

  - Auftragnehmer und Kunden
    - Persönliche Angaben wie Name, Titel, Position, Abteilung, Geschäftsbereich;
    - Kontaktangaben wie E-Mail-Adresse, Telefonnummer(n);
    - Arbeitsort;
    - Steuerinformationen wie Umsatzsteuer-Identifikationsnummern und Steuernummern

- „Verarbeitung" bezeichnet die Erhebung, Verwendung, Aufzeichnung, Organisierung, Änderung, Offenlegung, Vernichtung oder Speicherung personenbezogener Daten in jeglicher Form. Verarbeitung kann entweder manuell oder unter Einsatz automatisierter Systeme wie Informationstechnologiesysteme stattfinden, und „verarbeiten" und „Verarbeitung" werden entsprechend interpretiert.

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).

Anhang II
Datenschutzbeauftragter

Name: Maarten Veen
Funktion: Finanz-Direktor Heras Deutschland GmbH
Vollmacht: Gesamt-Prokura
E-Mail: m.veen@tmpp-group.com

[1] In dieser Richtlinie wird jeweils des Maskulinums verwendet, dies erfolgt zur besseren Lesbarkeit neutral für alle Geschlechter (m/w/d).