Heraeus

Merkblatt zur
Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Dieses Merkblatt gibt Ihnen die Möglichkeit, das Wichtigste zum Datenschutz nachzulesen. Sollten Sie Fragen haben – insbesondere, wenn es darum geht, ob ein bestimmter Umgang mit personenbezogenen Daten erlaubt ist –, wenden Sie sich bitte an Ihren Vorgesetzten oder Ihren Datenschutzkoordinator oder den betrieblichen Datenschutzbeauftragten. Die Kontaktdaten des Datenschutzbeauftragten finden Sie in Heraeus Touch (Heraeus Touch/ Unser Unternehmen/Funktionen/Legal & Responsibility/Data Protection).[1]

Datenschutz schützt auch Ihr Persönlichkeitsrecht

Das Datenschutzrecht dient nicht dem Schutz von Daten, sondern dem Persönlichkeitsrecht der Menschen, auf die sich die personenbezogenen Daten beziehen. Diese Menschen werden im Datenschutzrecht „Betroffene“ oder „betroffene Personen“ genannt. Das sind vor allem Ihre Kollegen, aber auch Sie selbst als Mitarbeiter können eine betroffene Person sein.

Das Persönlichkeitsrecht ist durch das Grundgesetz geschützt. Aus Art. 2 Abs. 1 GG (freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 GG (Würde des Menschen) hat das Bundesverfassungsgericht ein Grundrecht auf informationelle Selbstbestimmung abgeleitet, dass sich auch in Art. 8 der europäischen Grundrechtscharta wiederfindet. Das Recht auf informationelle Selbstbestimmung besagt, dass jeder Mensch in der Lage sein muss, darüber zu entscheiden, wer über seine personenbezogenen Daten verfügt und zu welchen Zwecken dies erfolgt. Das Recht auf informationelle Selbstbestimmung erfasst somit sämtliche Daten mit Personenbezug und betrifft alle Formen ihrer Erhebung und Verwendung. Es ist ein rechtliches Gegengewicht zur Entwicklung moderner Informationstechnologien und deren Möglichkeiten zur Verarbeitung von Daten.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist deshalb nur zulässig, wenn der Betroffene einwilligt oder ein Gesetz eine Verarbeitung personenbezogener Daten zulässt. Wichtige gesetzliche Erlaubnistatbestände sind in Art. 6 Abs. 1 DS-GVO enthalten. So besteht beispielsweise nach Art. 6 Abs. 1 b) DS-GVO die Erlaubnis, personenbezogene Daten zu verarbeiten, wenn dies für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich ist oder nach Art. 6 Abs. 1 c) DS-GVO, wenn die Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist.

[1] Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt; ungeachtet dessen beziehen sich die Angaben auf Angehörige aller Geschlechter.

Merkblatt zur
Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Die DS-GVO enthält keine explizite Regelung des Beschäftigtendatenschutzes. Deutschland hat die DS-GVO zum Anlass genommen, ein neues Bundesdatenschutzgesetz zu erlassen, das zusammen mit der DS-GVO am 25. Mai 2018 wirksam wird und das in § 26 BDSG die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses enthält. Diese gesetzliche Erlaubnisnorm ist im Wortlaut diesem Merkblatt beigefügt. Soweit dort auf die Verordnung (EU) 2016/679 Bezug genommen wird, ist damit die DS-GVO gemeint. § 26 Abs. 1 BDSG enthält die gesetzliche Erlaubnis, personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zu verarbeiten. Bitte beachten Sie, dass dies nicht nur die Arbeitnehmerinnen und Arbeitnehmer von Heraeus sind, sondern auch Leiharbeitnehmer/-innen, Bewerber/-innen auf ein Beschäftigungsverhältnis oder ehemalige Arbeitnehmerinnen und Arbeitnehmer Beschäftigte im Sinne von § 26 BDSG sind.

Was sind personenbezogene Daten?

Das Datenschutzrecht gilt nur für „personenbezogene Daten“. Technische und kaufmännische Informationen, die sich auf juristische Personen beziehen, unterliegen grundsätzlich nicht dem Datenschutz. Juristische Personen haben keine Persönlichkeit und müssen deshalb auch nicht geschützt werden. Der Personenbezug sollte aber nicht vorschnell verneint werden. Sobald nämlich der Bezug einer Information auf eine bestimmte oder bestimmbare natürliche Person hergestellt ist oder hergestellt werden kann, liegt ein personenbezogenes Datum vor. Beispielsweise sind IP-Adressen zunächst rein technische Angaben, die benötigt werden, um Absender- und Zieladressen bei einer Internet-Kommunikation zu identifizieren. Wenn eine solche IP-Adresse aber einem bestimmten Rechner und der Rechner einer natürlichen Person zugeordnet werden kann, ist ein Personenbezug gegeben. Aber auch dann, wenn eine IP-Adresse einem bestimmten Rechner nicht fest zugeordnet werden kann, durch einen Access-Provider aber das Datum, der Zeitpunkt und die Dauer einer Internetverbindung sowie die Teilnehmer dieser Internetverbindung ermittelt werden können, ist ein Personenbezug möglich. Dieses Beispiel soll Ihnen zeigen, dass ein Personenbezug auch dort möglich ist, wo dies auf den ersten Blick nicht der Fall zu sein scheint. Im Zweifelsfall sollten Sie deshalb von einem Personenbezug von Daten ausgehen.

Die gleiche Problematik stellt sich bei der Abgrenzung von anonymen und pseudonymen Daten. Anonyme Daten unterliegen nicht dem Datenschutz. Voraussetzung für eine Anonymisierung ist jedoch, dass ein Personenbezug nicht mehr hergestellt werden kann. Kann ein solcher Personenbezug unter Hinzuziehung zusätzlicher Informationen und ggf. weiterer technischer oder organisatorischer Maßnahmen wiederhergestellt werden, liegen sogenannte pseudonyme Daten vor, die dem Datenschutz unterliegen. Auch hier sollten

Sie in Zweifelsfällen davon ausgehen, dass keine anonymen, sondern nur pseudonyme Daten vorliegen. Fragen Sie bei Unklarheiten Ihren Datenschutzkoordinator oder den betrieblichen Datenschutzbeauftragten.

Gilt der Datenschutz nur für Computer-Daten?

Nein, das Datenschutzrecht gilt auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Das Datenschutzrecht findet somit auch Anwendung auf die alphabetische Sammlung ausgefüllter Papierformulare oder Beschäftigtenkarteien auf Papier.

Beachten Sie bitte, dass der Beschäftigtendatenschutz in Deutschland Daten von Beschäftigten auch dann schützt, wenn diese nur manuell erhoben und nicht in einer Datei gespeichert sind oder gespeichert werden sollen. Dem deutschen Datenschutzrecht unterfällt somit auch jede handschriftliche Notiz über Beschäftigte, auch wenn diese Notizen unsortiert sind und auch unsortiert bleiben sollen. Dieser Hinweis ist vor allem wichtig für die datenschutzgerechte Löschung und Entsorgung. Wenn Sie im Rahmen eines Bewerbergesprächs oder sonstigen Besprechungen handschriftliche Notizen anfertigen, die personenbezogene Daten von Beschäftigten enthalten, müssen diese personenbezogenen Daten unverzüglich in die entsprechenden Datenbanken eingepflegt werden. Nachdem dies geschehen ist, besteht keine Notwendigkeit mehr, handschriftliche Notizen länger aufzubewahren. Diese handschriftlichen Notizen müssen deshalb „gelöscht“ werden. Diese Löschung geschieht dadurch, dass Sie diese datenschutzgerecht vernichten.

Das Wegwerfen von handschriftlichen Notizen in Papiereimer ist keine datenschutzgerechte Entsorgung!

Bitte entsorgen Sie alle Papiere, die Beschäftigtendaten enthalten, ausschließlich über die dafür vorgesehenen Papierentsorgungscontainer, die durch Schlösser gegen Öffnen gesichert sind. Erkennen Sie, dass ein Papierentsorgungscontainer nicht durch Schlösser gesichert ist, darf in einen solchen Container, kein Papier entsorgt werden, auf dem sich Beschäftigtendaten oder sonstige personenbezogenen Daten befinden.

Welche Rechte haben die betroffenen Personen?

Die betroffenen Personen haben zunächst das Recht, darüber informiert zu werden, welche Daten über sie gespeichert sind und zu welchen Zwecken sie verarbeitet und wann sie wieder gelöscht werden. Diesem Informationsrecht der betroffenen Personen entspricht

eine Informationspflicht der Verantwortlichen. Verantwortliche sind aber nicht Sie, sondern Heraeus. Bitte verwenden Sie zur Information der betroffenen Personen ausschließlich des Informationsmaterials, das Ihnen Heraeus für diesen Zweck zur Verfügung stellt.

Neben dem Anspruch auf Information haben die betroffenen Personen auch einen Anspruch auf Auskunft. Die Pflicht, diese Auskunft zu geben und der betroffenen Person Kopien ihrer Daten zur Verfügung zu stellen, obliegt Heraeus und nicht Ihnen. Zur Erfüllung dieser Auskunftsansprüche stellt Heraeus ein Verfahren zur Verfügung und benennt Mitarbeiter, die für die Durchführung dieses Auskunftsverfahrens zuständig sind. Geben Sie bitte keine Auskünfte, wenn Sie nicht zu diesem Personenkreis gehören. Das Erteilen einer Auskunft ist eine Datenübermittlung, die rechtswidrig ist, wenn sie ohne Erlaubnis erfolgt. Verweisen Sie deshalb Personen, die einen Auskunftsanspruch nach Datenschutzrecht geltend machen, an die hierfür zuständigen Stellen bei Heraeus.

Die betroffenen Personen haben auch einen Anspruch, dass falsche Daten über sie berichtigt oder nicht mehr benötigte Daten über sie gelöscht werden. Diese Pflicht obliegt aber Heraeus und nicht Ihnen. Berichtigen oder löschen Sie Daten nur auf Anweisung der hierfür zuständigen Personen bei Heraeus. Auf Bitten der betroffenen Person dürfen Daten nur berichtigt oder gelöscht werden, wenn diese einen entsprechenden Nachweis erbringt. Sollten Sie selbst feststellen, dass nicht mehr benötigte Daten weiterhin gespeichert bleiben oder gespeicherte Daten falsch oder unrichtig geworden sind, sprechen Sie bitte Ihren Vorgesetzten oder den Datenschutzkoordinator oder den betrieblichen Datenschutzbeauftragten hierauf an.

Die Speicherung von Daten, die eigentlich zu löschen wären, kann mit Geldbußen bis € 20.000.000,00 oder 4 % des weltweiten Jahresumsatzes des gesamten Konzerns – je nach dem, was höher ist – bestraft werden. Zusätzlich haben betroffene Personen Anspruch auf Schadenersatz einschließlich Schmerzensgeld für die Verletzung ihres Persönlichkeitsrechts. Bitte melden Sie Ihrem Vorgesetzten oder dem Datenschutzkoordinator umgehend, wenn Sie einen solchen Umstand entdecken und beachten Sie bitte, dass auch die datenschutzgerechte Entsorgung handschriftlicher Notizen oder sonstiger Papierdokumente unter den Löschungsanspruch der Betroffenen fällt. Gerade in der täglichen Kommunikation per E-Mail oder bei Kalendereinträgen mit Anhang ist dieser Löschungsanspruch ebenso wichtig und kontinuierlich zu beachten und zu realisieren.

Sollte ein Auskunftsersuchen, ein Widerspruch oder ein anderer Wunsch oder Hinweis mit Datenschutzbezug bei Ihnen eingehen, leiten Sie ihn bitte umgehend an Ihren Vorgesetzten und den Datenschutzkoordinator Ihres Bereichs oder den betrieblichen

Datenschutzbeauftragten weiter. Das gilt auch bei Anfragen von Behörden, der Polizei oder der Staatsanwaltschaft.
Selbständig dürfen Sie solche Anfragen nur bearbeiten, wenn Heraeus Ihnen diese Aufgabe ausdrücklich zugewiesen hat. In Zweifelsfällen fragen Sie Ihren Vorgesetzten oder den Datenschutzkoordinator Ihres Bereichs.

Neue Datenverarbeitungsverfahren

Sollten Sie an einem Projekt beteiligt sein, bei dem personenbezogene Daten eine Rolle spielen oder bei dem neue Verarbeitungsverfahren eingeführt werden, sollten Sie den betrieblichen Datenschutzbeauftragten frühzeitig einbeziehen. Er kann Ihnen sagen, ob es überhaupt rechtlich zulässig ist, was geplant wird und Tipps geben, was Sie verbessern können, insbesondere welche Anforderungen einzuhalten sind im Hinblick auf „Privacy by Design“, „Privacy by Default“ und Datensicherheit. Wenn Sie diese Fragen rechtzeitig mit dem betrieblichen Datenschutzbeauftragten klären, können Sie von Anfang an das richtige Verfahren entwickeln. Wenn Sie ihn erst kurz vor Schluss einbeziehen, kann es sein, dass Ihr Projekt aus datenschutzrechtlichen Gründen scheitert oder zeitlich erheblich verzögert wird.

Sie sind verpflichtet, neue Datenverarbeitungsverfahren rechtzeitig zu melden, damit Heraeus seiner Pflicht nachkommen kann, eine vollständige Dokumentation sämtlicher Datenverarbeitungen vorzuhalten. Bitte verwenden Sie für die Meldung neuer Datenverarbeitungsverfahren die von Heraeus hierfür vorgesehenen IT-Tools. Weitere Hinweise dazu können Sie dem Intranet unter Datenschutz entnehmen.

Besondere Hinweise für die Nutzung von Internet und E-Mail

Bitte beachten Sie, dass eine private Nutzung Ihres E-Mail Accounts bei Heraeus nicht gestattet ist.

Vertrauliche Daten, insbesondere sensible personenbezogene Daten von Beschäftigten, dürfen nur datenschutzgerecht versendet werden. Wenn Ihr Computer mit einem Programm zur E-Mail-Verschlüsselung ausgestattet ist und der Empfänger der E-Mail ebenfalls so ein Programm verwendet, dürfen Sie sensible personenbezogene Daten von Beschäftigten nur mit verschlüsselter E-Mail versenden.

Sollten Sie kein Programm zur E-Mail-Verschlüsselung haben, dürfen besonders sensible Daten wie Lohn- und Gehaltsdaten nur in einem verschlüsselten Anhang oder in einer E-Mail mit Kennzeichnung „privat“ oder per Hauspost in einem verschlossenen Umschlag mit

dem Vermerk „Persönlich/Vertraulich“ versendet werden. Eine telefonische Übermittlung besonders sensibler Daten ist weiterhin möglich. Insgesamt ist bei der E-Mail-Kommunikation mit sensiblen personenbezogenen Daten stets soweit möglich die Kennzeichnung „privat“, aber mindestens „vertraulich“ zu wählen.

Bevor Sie eine E-Mail versenden, sollten Sie stets darauf achten, dass der richtige Empfänger im Adressfeld steht. Bei gleichen oder ähnlichen Namen oder E-Mail-Adressen kann es leicht zu Verwechslungen kommen. Kontrollieren Sie deshalb vor dem Abschicken, ob nur befugte Empfänger im Adressfeld stehen. Eine Verwechslung oder Unachtsamkeit kann zu schwerwiegenden Datenpannen führen, wenn besonders sensible Daten von Beschäftigten an Empfänger gelangen, die für diese nicht bestimmt waren. Bitte beachten Sie ferner, dass jeder Empfänger auch Kenntnis erlangt, wer diese E-Mail sonst noch empfangen hat. Wenn Sie E-Mails an mehrere Empfänger absenden, vergewissern Sie sich deshalb, dass nicht nur alle Empfänger empfangsberechtigt sind, sondern auch Kenntnis vom Empfängerkreis haben dürfen.

E-Mails mit persönlichem/vertraulichem Inhalt an den Betriebsrat, den Betriebsarzt oder die Sozialberatung sollten Sie nach Möglichkeit vermeiden oder nur in verschlüsselten Anhängen versenden. Sollte es sich ausnahmsweise nicht vermeiden lassen, sensible personenbezogene Daten per E-Mail zu versenden, sollten Sie solche E-Mails möglichst umgehend von Ihrem E-Mail-Account entfernen, entweder durch Löschen oder durch Verschieben in passwortgeschützte Dateien, die nur für Sie zugänglich sind.

Bei Datenpannen existieren gesetzliche Meldepflichten. Nicht jeder Datenschutzverstoß stellt eine Datenpanne dar, sondern es müssen besonders kritische Daten von dem Verstoß betroffen sein und schwerwiegende Beeinträchtigungen für die Rechte oder die schutzwürdigen Interessen der Betroffen drohen. Sollte Sie eine Datenpanne feststellen oder vermuten, informieren Sie bitte umgehend Ihren Vorgesetzten und den Datenschutzkoordinator Ihres Bereichs oder den betrieblichen Datenschutzbeauftragten.

Es ist Ihnen untersagt, E-Mails mit vertraulichen Daten an Ihren privaten E-Mail-Account weiterzuleiten oder woanders als auf den hierfür vorgesehen Servern von Heraeus zu speichern. Dies bedeutet, dass Sie auf keinen Fall eine automatische Weiterleitung Ihres E-Mail-Accounts an Ihre private E-Mail-Adresse einrichten dürfen.

Sie werden möglicherweise E-Mails erhalten, die Sie im Namen von anderen Unternehmen oder möglicherweise sogar im Namen von Heraeus auffordern, auf einen Link in der E-Mail zu klicken oder eine bestimmte Seite aufzurufen oder dort Ihr Passwort oder andere Daten einzugeben. Prüfen Sie stets, ob der Absender vertrauenswürdig ist und die E-Mail auch

tatsächlich von ihm kommt. Selbst wenn Sie in einer solchen E-Mail persönlich angesprochen werden oder gar Bezug auf bestimmte Personen oder Umstände genommen wird, bedeutet dies nicht, dass die E-Mail vertrauenswürdig ist. Absenderangaben von E-Mails lassen sich problemlos fälschen. Seien Sie daher bitte auch sehr vorsichtig, wenn Sie unaufgefordert E-Mails mit Anhängen (Attachments) erhalten. Bevor Sie einen solchen Anhang öffnen, fragen Sie bitte im Zweifel bei IT-Helpdesk nach. Seien Sie auch misstrauisch, wenn als Absender Ihr Vorgesetzter oder andere Führungskräfte von Heraeus oder gar Geschäftsführer von Heraeus unter Hinweis auf besondere Vertraulichkeit Handlungen von Ihnen verlangen, die in Widerspruch zu internen Heraeus-Richtlinien stehen. Gehen Sie davon aus, dass Geschäftsführer, Führungskräfte und Vorgesetzte von Ihnen keine Handlungen per E-Mail oder auf anderem Weg verlangen, die im Widerspruch zu Heraeus-internen Richtlinien stehen. Fragen Sie in jedem Fall auf einem anderen Kommunikationskanal beim vermeintlichen Absender an, ob die betreffende E-Mail von ihm stammt.

Sollten Sie unerbetene private E-Mails auf Ihrem Heraeus E-Mail-Account empfangen, sollten Sie diese E-Mails umgehend löschen.