

Datenschutzgrundsätze in Vergabeverfahren

Im Rahmen von Vergabeverfahren wird empfohlen, datenschutzrechtliche Grundsätze zu beachten.

Explizit bei der **Beschaffung von Verfahren**, die im weiteren Verlauf dazu dienen, personenbezogene Daten zu verarbeiten, wird empfohlen, dem Grundsatz des „**Privacy by Design/ by Default**“ nach [Art. 25 DSGVO](#) zu entsprechen. Was bedeutet das?

Was versteht man unter Privacy by Default und Privacy by Design?

Die datenschutzfreundliche Technikgestaltung und datenschutzfreundliche Voreinstellungen, welche in diesem Zusammenhang mit Privacy by Design und Privacy by Default umschrieben werden, sind in [Art. 25 DSGVO](#) geregelt. Darin wird gemäß dem in der DSGVO verankerten risikobasierten Ansatz gefordert, angemessene und verhältnismäßige, aber dennoch robuste Maßnahmen zum Schutz personenbezogener Daten umzusetzen. Bei der Abwägung über die Maßnahmen im Einzelfall wird eine Datenschutz-Folgenabschätzung notwendig, die gegenüber den Aufsichtsbehörden gem. [Art. 5 Abs. 2 DSGVO](#) auch dokumentiert sein muss.

Privacy by Default

In [Art. 25 Abs. 2 DSGVO](#) ist die Pflicht zu Privacy by Default geregelt, die besagt, dass übertragen auf ein Anwendungsprodukt, dieses nur eingesetzt werden darf, wenn die Anwendung so ausgelegt ist, dass ohne weitere Aktivität des Nutzers die datenschutzfreundlichsten Einstellungen eingerichtet sind. Damit soll erreicht werden, dass nur die für den jeweiligen Verarbeitungszweck erforderlichen personenbezogenen Daten verarbeitet werden und dem Datenminimierungsgrundsatz Rechnung getragen wird.

Privacy by Design

Die datenschutzfreundliche Technikgestaltung (Privacy by Design) wiederum ist in [Art. 25 Abs. 1 DSGVO](#) geregelt. Damit soll erreicht werden, dass auf den Einzelfall bezogen, risikobasiert, effektive und angemessene technische sowie organisatorische Maßnahmen ergriffen werden. Zum einen sollen die Maßnahmen die Einhaltung der wesentlichen datenschutzrechtlichen Grundsätze aus [Art. 5 Abs. 1 DSGVO](#) sicherstellen, wie:

- Zweckbindung
- Rechtmäßigkeit
- Datenminimierung
- Transparenz
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Treu und Glauben
- Richtigkeit

Zum anderen sollen die Maßnahmen aber auch hinreichende Garantien für die Rechte der Betroffenen und die Einhaltung der Pflichten aus der DSGVO enthalten. Die getroffenen Maßnahmen müssen die Einhaltung der Grundsätze aus [Art. 5, 24 DSGVO](#) garantieren.

Es reicht, wenn die Technikgestaltung effektiv ist und im Wege einer schriftlichen Dokumentation gem. [Art. 5 Abs. 2 DSGVO](#) nachgewiesen werden kann.

Wann sollte die datenschutzfreundliche Technikgestaltung berücksichtigt werden?

Sinnvollerweise wird die Datenschutzfreundlichkeit bereits zu einem sehr frühen Zeitpunkt bei der Herstellung des jeweiligen Verfahrens berücksichtigt. [Art. 25 DSGVO](#) beschreibt hierzu, dass die Schutzmaßnahmen bei der Festlegung der Mittel, also bereits bei der Entwicklung und der Konzeption des Verfahrens sowie zum Zeitpunkt der Verarbeitung, also über den gesamten Lebenszyklus des Produkts hinweg, bedacht und implementiert werden sollte. Gerade bei der Anwendungsentwicklung sollten diese Grundsätze bei jedem Update gleichfalls berücksichtigt werden. **Die Verfahren, die im Rahmen einer Vergabe erworben werden, sollten diese Anforderungen also schon erfüllen.**

Wer ist für die DSGVO-konforme Technikgestaltung zuständig?

[Art. 25 DSGVO](#) stellt in Abs. 1 und 2 ausdrücklich auf den **Verantwortlichen** ab. Datenschutzrechtlich verantwortlich und zuständig für die DSGVO-konforme Technikgestaltung ist der Kreis Herford. Die Umsetzungsverantwortung liegt in der Kreisverwaltung Herford bei den Abteilungs-, Betriebs-, Einrichtungs-, Fachbereichs- und Stabsbereichsleitungen.

Ein Verfahren¹, mit dem personenbezogene Daten verarbeitet werden (sollen), muss daher den Datenschutz berücksichtigen. **Der Verantwortliche sollte sich nach der Orientierungshilfe „[Datenschutz als Kriterium im Vergabeverfahren des Bayerischen Landesbeauftragten für Datenschutz vom 01.02.2024](#)“ davon bereits vor Einleitung des Beschaffungsvorgangs vergegenwärtigen.**

Im Rahmen der Vergabe von Verfahren, die in den Sozialbereichen des Kreises Herford eingesetzt werden sollen, ist darüber hinaus [§ 80 Abs. 2 SGB X](#) zu beachten. Hiernach dürfen personenbezogene Daten nur...

- innerhalb der EU
 - in einem nach [§ 35 Abs. 7 SGB I](#) gleichgestellten Staat
 - in einem Staat, für den ein [Angemessenheitsbeschluss](#) vorliegt
- verarbeitet werden.

Es muss allen Verantwortlichen beim Kreis Herford klar sein, dass eine Anwendung, die einem bestimmten Verwendungszweck dienen soll, und mit der personenbezogene Daten verarbeitet werden (sollen), folgende elementare Technikeinstellungen aufweisen muss:

- Die Möglichkeit Einwilligungen inkl. deren Widerruf entsprechend der Vorgaben aus der DSGVO zu erfassen und die Daten zu löschen.
- Das Erfassen von Widersprüchen.
- Die Gewährung von Datenkopien und Datenübertragbarkeit.
- Die Zurverfügungstellung von Betroffeneninformationen für das Verfahren, damit diese von dem Verfahrensanwender für die Datenschutzerklärung oder andere eigene Betroffeneninformationen verwendet werden können.
- Eine Dokumentation, an welchen Stellen die personenbezogenen Daten verarbeitet werden.
- Eine Löschfunktion für die verarbeiteten personenbezogenen Daten über alle Bereiche hinweg (inkl. Archive) zusammen mit der Möglichkeit dies zu automatisieren - inkl. Freigabefunktionalitäten.
- Ein Rollen- und Berechtigungskonzept.
- Die Möglichkeit Daten zu pseudonymisieren und zu anonymisieren.

Die vergebenden Stellen beim Kreis Herford sollten gleichermaßen darauf achten, dass die Verfahren, mit denen personenbezogene Daten verarbeitet werden (sollen), den oben angeführten Mindestanforderungen entsprechen und Dokumentationen nach [Art. 5 Abs. 2 DSGVO](#) vorgenommen werden können, um der Rechenschaftspflicht nachzukommen.

¹ Unabhängig von einer „On Premise – Lösung“ oder einer „SaaS-Lösung“

Unter Berücksichtigung dieser Erläuterungen wird aus datenschutzrechtlicher Sicht empfohlen, den nachfolgenden Text in die Vergabeunterlagen (Vorbemerkungen/ Leistungsbeschreibung) aufzunehmen, aber auch bei freihändigen Vergaben anzuwenden, und diese zum Bestandteil des Auftrags zu machen:

**Beginn Textpassage für die Vergabe von Verfahren,
mit denen personenbezogene Daten verarbeitet werden sollen**

Datenschutz

Im Rahmen der zukünftigen Zusammenarbeit sind folgende Vorgaben zu beachten:

1. Die Bieterin/ Der Bieter sichert gegenüber dem Auftraggeber Kreis Herford die Einhaltung und Umsetzung der DSGVO, des DSG NRW und soweit zutreffend des BDSG, des DDG und des TDDDG schriftlich zu, - dies kann auch durch Nachweis einer Zertifizierung geschehen.
2. Die Bieterin/ Der Bieter stellt dem Auftraggeber auf Anforderung vor der Einführung eines elektronischen Verfahrens/ der geplanten Auftragsverarbeitung, mit dem/ im Rahmen derer personenbezogene Daten verarbeitet werden (sollen), vor der Auftragsvergabe ihre/ seine datenschutzrechtliche Dokumentation und erforderlichen Informationen zur Erstellung einer eigenen datenschutzrechtlichen Dokumentation zur Verfügung.
3. Die Bieterin/ Der Bieter belegt gegenüber dem Auftraggeber Kreis Herford auf Anforderung die Umsetzung des Datenschutzes durch Vorlage folgender Dokumente:
 - Entwurf des abzuschließenden Auftragsverarbeitungsvertrages nach [Art. 28 Abs. 3 DSGVO](#) (inhaltlich entsprechend der [Empfehlungen der Datenschutzaufsichtsbehörden](#) der Länder und des Bundes).
Alternativ stellt der Kreis Herford für die Auftragsverarbeitung ein Muster des Auftragsverarbeitungsvertrages entsprechend der Empfehlungen der Datenschutzaufsichtsbehörden der Länder und des Bundes zur Verfügung.
 - Nachweis von Zertifizierung(en), soweit vorhanden (ISO/IEC 27001 oder ISO/IEC 27002 oder nach Inkrafttreten ISO/IEC DIS 27701 oder Art. 42 DSGVO) des eigenen oder des fremden Rechenzentrums, in denen die personenbezogenen Daten verarbeitet werden sollen.
 - Nachweis über getroffene technische- und organisatorische Maßnahmen nach [Art. 32 DSGVO](#), zum Schutz der im Auftrag zu verarbeitenden personenbezogenen Daten.
 - Bei Nutzung eines Rechenzentrums, dessen Muttergesellschaft ihren Hauptsitz in einem Drittland (z.B. USA) hat, Nachweis, mit welchen konkreten Maßnahmen der [Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 31. Januar 2023](#) umgesetzt worden ist/wird.
 - Verzeichnis von Verarbeitungstätigkeiten nach [Art. 30 DSGVO](#) für das Verfahren, mit dem die personenbezogenen Daten für den Kreis Herford verarbeitet werden sollen.
 - Datenschutz-Folgenabschätzung nach [Art. 35 DSGVO](#) oder Erklärung, weshalb keine Datenschutz-Folgenabschätzung für die beabsichtigte Verarbeitung der personenbezogenen Daten erforderlich ist, zumindest den Nachweis über eine durchgeführte Schwellwertanalyse mit entsprechendem Ergebnis.
 - Alle involvierten Mitarbeiter*innen der Bieterin/ des Bieters müssen zur Verschwiegenheit verpflichtet sein. Die Bieterin/ der Bieter sichert schriftlich zu, regelmäßige Datenschutz-Unterweisungen anzubieten und kann diese auf Anforderung im Rahmen der Kontrolle nach [Art. 28 \(3\) DSGVO](#) vorlegen.
4. Die vorgenannten Angaben sind Voraussetzung für die Berücksichtigung des eingereichten Angebotes im Rahmen des jeweiligen Ausschreibungsverfahrens.

5. Über die ausgeschriebene Leistung ist mit der Bieterin/ dem Bieter ein Vertrag, im Auftragsverarbeitungsvertrag wird von einem Hauptvertrag gesprochen, abzuschließen, da dieser Vertrag aus datenschutzrechtlicher Sicht eine Ergänzung zum Auftragsverarbeitungsvertrag darstellt.
6. Die Einwilligung der Bieterin/ des Bieters zur Datenverarbeitung durch den Kreis Herford wird mittels Kenntnisnahme der Datenschutzinformation nach Artikel 13/14 Datenschutz-Grundverordnung (Verordnung (EU) 2016/679 vom 27. April 2016) erklärt².

Hinweis:

Unternehmen haben alle für sie geltenden rechtlichen Verpflichtungen einzuhalten. Dies umfasst alle zwingenden Rechtsvorschriften und damit auch die zwingenden Teile der Datenschutz-Grundverordnung (DSGVO). Ein Verstoß gegen die rechtliche Verpflichtung kann unterhalb der Strafbarkeitsschwelle einen fakultativen Ausschlussgrund vom Verfahren im Sinne § 124 (1) GWB, § 57 (1) VgV wegen mangelnder Eignung begründen.

Verstöße gegen datenschutzrechtliche Bestimmungen können dabei eine „nachweisliche schwere Verfehlung im Rahmen der beruflichen Tätigkeit“ darstellen, § 124 (1) Nr. 3 GWB. Ebenso kommt bei Nichtbeachtung von zwingenden Datenschutzvorhaben ein Ausschluss gemäß §§ 53 (7), 57 (1) Nr. 4 VgV wegen Änderung der Vertragsunterlagen in Betracht.

**Ende der Textpassage für die Vergabe von Verfahren,
mit denen personenbezogene Daten verarbeitet werden sollen**

Die von der im Ausschreibungsverfahren obsiegenden Bieterin/ vom obsiegenden Bieter angeforderten und vorgelegten datenschutzrechtlichen Dokumente sollten datenschutzrechtlich auf inhaltliche Vollständigkeit geprüft werden.

Die Verantwortung der datenschutzrechtlichen Prüfung der durch die Bieterin/ des Bieters vorgelegten Dokumente, trägt in förmlichen Vergabeverfahren die für die Vergabestelle des Kreises Herford verantwortliche Führungskraft und bei freihändigen Vergaben die örtlich verantwortliche Führungskraft.

Die/ Der Datenschutzbeauftragte bietet in diesem Zusammenhang ihre/ seine Unterstützung an.

² Diese Informationen werden bei der Veröffentlichung durch die Zentrale Vergabestelle beigelegt