

### **Abgrenzung der Anwendungsbereiche von Datenschutz-Grundverordnung (DSGVO) oder der Richtlinie (EU) 2016/680 Polizei/Justiz (DS-RL)**

BMI haben verschiedene Anfragen aus den Ländern und dem Ressortkreis erreicht, unter welches Datenschutzregime (DSGVO oder DS-RL) Datenverarbeitungen zum Zweck der Gefahrenabwehr fallen, insbesondere wenn nicht die Polizei, sondern die Ordnungsbehörden tätig werden.

Die DS-RL (in Artikel 1 Absatz 1 und Artikel 2 Absatz 1) sowie spiegelbildlich die DSGVO (in Artikel 2 Absatz 2 Buchstabe d) grenzt die Anwendungsbereiche der beiden Regelungsregime ab. Nach Artikel 1 Absatz 1 DS-RL und spiegelbildlich Artikel 2 Absatz 2 Buchstabe d DSGVO umfasst der sachliche Anwendungsbereich der DS-RL *„die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“*. Zugleich setzt Artikel 2 Absatz 1 DS-RL neben der Verarbeitung zu den zuvor genannten spezifischen Zwecken eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit voraus. Insbesondere die Formulierung *„einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“* wirft Auslegungsfragen auf, ob der Anwendungsbereich der DS-RL nur die straftatenbezogene oder auch die nicht straftatenbezogene Gefahrenabwehr umfassen soll.

BMI kommt in Übereinstimmung mit BMJV zu folgendem Ergebnis:

1. Der Anwendungsbereich der DS-RL umfasst nur die straftatenbezogene Gefahrenabwehr durch die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständigen Behörden. Die Verarbeitung personenbezogener Daten durch die Polizei oder die Ordnungsbehörden im Rahmen der nicht straftatenbezogenen Gefahrenabwehr unterliegen dem Anwendungsbereich der DSGVO.

Dieses Verständnis hat auch der Bundesgesetzgeber im Rahmen der Anpassung des Datenschutzrechts an die DSGVO und die DS-RL durch das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG EU) vom 30. Juni 2017 (BGBl. I S. 2097) zugrunde gelegt. § 45 Satz 1 BDSG 2018, der Artikel 1 Absatz 1 und Artikel 2 Absatz 1 DS-RL umsetzt, bezieht den Anwendungsbereich des Dritten Teils des BDSG 2018 und damit der DS-RL auf *„die*

*Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten*“. Für den Bereich der Gefahrenabwehr konkretisiert § 45 Satz 3 BDSG 2018 den Anwendungsbereich wie folgt: *„Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit“*. Die Verhütung von Ordnungswidrigkeiten oder allgemein die Abwehr von Gefahren für die öffentliche Sicherheit werden in § 45 Satz 3 BDSG 2018 nicht erwähnt. Daraus folgt, dass Bereiche der Gefahrenabwehr, die keinen Bezug zu Straftaten aufweisen, nicht vom Anwendungsbereich der DS-RL bzw. des diesen umsetzenden Dritten Teils des BDSG umfasst sind.

Dieses enge Verständnis lag auch dem Entwurf des Datenschutzanpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) zugrunde. Nach der Begründung des Gesetzentwurfs (BT-Drs. 18/11325, S. 110) sollte der die DS-RL umsetzende Dritte Teil des BDSG 2018 nur gelten *„für Verarbeitungen durch öffentliche Stellen und [...] als öffentliche Stellen geltende Beliehene, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten [...], einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind, und auch nur, soweit sie zu diesen Zwecken Daten verarbeiten“*. Dies deckt sich auch mit der Auffassung der EU-Kommission, die sich in einem Schreiben der Justizkommissarin Eva Jourova vom 8. Mai 2017 im Zuge der anstehenden Beschlussfassung des Bundesrates zum DSAnpUG-EU wie folgt positioniert hat: *„Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke ‚des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit‘ (Artikel 1 Absatz 1 der Polizei-Richtlinie) fällt nur dann in den Anwendungsbereich der Polizei-Richtlinie, wenn sie im Rahmen der Tätigkeiten dieser Behörden im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung erfolgt.“*

Um festzustellen welches Datenschutzregime anzuwenden ist, ist eine Einzelfallprüfung erforderlich, ob

- a) die Tätigkeit der handelnden Behörde (Polizei oder Ordnungsbehörde) auf die straftatenbezogene oder die nicht straftatenbezogene Gefahrenabwehr ausgerichtet ist und
- b) die handelnde Behörde für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständig ist.

2. Aufgrund der spezifischen Zuständigkeit der Polizeibehörden für die Kriminalitätsbekämpfung ist bei polizeilichen Gefahrenabwehrmaßnahmen regelmäßig von einem Straftatenbezug und damit von der Geltung der DS-RL auszugehen. Dies gilt auch für polizeiliche Tätigkeiten, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht.

Dies wird insbesondere durch Erwägungsgrund 12 DS-RL unterstützt: *„Die Tätigkeiten der Polizei oder anderer Strafverfolgungsbehörden sind hauptsächlich auf die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten ausgerichtet, dazu zählen auch polizeiliche Tätigkeiten in Fällen, in denen nicht von vornherein bekannt ist, ob es sich um Straftaten handelt oder nicht. Solche Tätigkeiten können ferner die Ausübung hoheitlicher Gewalt durch Ergreifung von Zwangsmitteln umfassen, wie polizeiliche Tätigkeiten bei Demonstrationen, großen Sportveranstaltungen und Ausschreitungen. Sie umfassen auch die Aufrechterhaltung der öffentlichen Ordnung als Aufgabe, die der Polizei oder anderen Strafverfolgungsbehörden übertragen wurde, soweit dies zum Zweck des Schutzes vor und der Abwehr von Bedrohungen der öffentlichen Sicherheit und Bedrohungen für durch Rechtsvorschriften geschützte grundlegende Interessen der Gesellschaft, die zu einer Straftat führen können, erforderlich ist.“*

Beispiele:

- Personenkontrollen durch die Polizei auf öffentlichen Plätzen (Kriminalitätsschwerpunkte);
  - Polizeiliche Maßnahmen im Zuge von Versammlungen (etwa Auflösung, Ausschluss von Teilnehmern, Festnahmen, Bild- und Tonaufnahmen von Versammlungen soweit sie der Aufklärung von Straftaten dienen);
  - Polizeiliche Maßnahmen zum Schutz vor Angriffen auf die Luftsicherheit (z. B. anlassbezogene Überprüfung von Personen im Sicherheitsbereich von Flughäfen).
3. In Fällen, in denen die Polizei Daten im Rahmen von Gefahrenabwehrmaßnahmen verarbeitet und in denen eindeutig kein Straftatenbezug gegeben ist, kann auch die polizeiliche Datenverarbeitung unter das Datenschutzregime der DSGVO fallen.

Dies wird insbesondere durch Erwägungsgrund 12 Satz 4 DS-RL unterstützt: *„Die Mitgliedstaaten können die zuständigen Behörden mit anderen Aufgaben*

*betrauen, die nicht zwangsläufig für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, ausgeführt werden, so dass die Verarbeitung von personenbezogenen Daten für diese anderen Zwecke insoweit in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt, als sie in den Anwendungsbereich des Unionsrechts fällt“.*

Beispiele:

- Die Polizei schreitet bei Selbstverletzungs- oder und Suizid-Fällen ein, bei denen Fremdeinwirkung eindeutig ausgeschlossen ist (d. h. nicht in Fällen eines unklaren Todesfalles).
  - Die Polizei wird zum Schutz privater Rechte im Sinne der Polizeigesetze tätig.
  - Die Polizei wird zur Abwehr von Gefahren für die öffentliche Ordnung im Rahmen ihrer „Eilzuständigkeit“ für die Ordnungsbehörde tätig.
4. Auf die Datenverarbeitung durch die gefahrenabwehrend tätigen Ordnungsbehörden (oder Polizeibehörden, soweit dort gefahrenabwehrende Aufgaben organisatorisch angesiedelt sind, wie teilweise etwa in Bereich des Versammlungsrechts der Länder) findet in der Regel das Datenschutzregime der DSGVO Anwendung. Dies gilt etwa für ordnungsrechtliche Prüf-, Anmelde-, Genehmigungs-, Erlaubnis- oder Zuverlässigkeitsverfahren einschließlich der zur Abwehr von Gefahren ausgesprochenen Anordnungen, Auflagen und Untersagungen aufgrund der jeweiligen allgemeinen oder spezialgesetzlichen Befugnisnormen. Diese weisen in der Regel nicht den erforderlichen Straftatenbezug auf, sondern dienen vorrangig der Abwehr und dem Schutz vor bestimmten Gefahrensituationen, die in der Regel spezialgesetzlich definiert sind. Die Verhütung von Straftaten steht typischerweise nicht im Vordergrund dieser Maßnahmen.

So hält das BMI in folgenden Fällen den Anwendungsbereich der DSGVO für eröffnet:

- Genehmigungsverfahren, etwa nach dem Bundesimmissionsschutzgesetz, der Gewerbeordnung oder dem Gaststättengesetz;
- Versammlungsrechtliches Anmeldeverfahren, auch wenn diese Aufgabe im jeweiligen Landesrecht ggf. der Polizei übertragen ist;

- Straßenverkehrsrechtliche Maßnahmen, etwa nach der Straßenverkehrsordnung;
- Erlaubnisverfahren nach dem Waffengesetz;
- Gewerberechtliche Maßnahmen nach dem Prostituiertenschutzgesetz;
- Anordnungen, Auflagen, Verbote, Untersagungen, Stilllegungen, Entziehungen u. ä. nach den jeweiligen Spezialgesetzen (etwa nach dem Arbeitsschutzgesetz, Waffengesetz, Versammlungsgesetz, Pass- und Personalausweisgesetz oder Bundesimmissionsschutzgesetz);
- Prüfungen der Behörden der Zollverwaltung und der sie unterstützenden Behörden nach dem Schwarzarbeitsbekämpfungsgesetz.

5. In Ausnahmefällen kann bei Datenverarbeitungen durch Ordnungsbehörden auch die DS-RL anwendbar sein. Denkbar ist dies in Gefahrenabwehrbereichen, in denen Sonderordnungsbehörden nicht nur für die Verhütung von Straftaten, sondern darüber hinaus auch für die Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständig sind.

So hält BMI den Anwendungsbereich der DS-RL etwa für folgende Bereiche für eröffnet:

- Maßnahmen der Verbotsbehörden im Rahmen vereinsrechtlicher Verbotverfahren nach dem Vereinsgesetz;
- Maßnahmen der Zentralstelle für Finanztransaktionsuntersuchungen nach dem Geldwäschegesetz.

6. Datenverarbeitungen zum Zwecke der Gefahrenabwehr, die nach den vorgenannten Grundsätzen dem Datenschutzregime der DSGVO unterliegen, fallen jedoch dann in den Anwendungsbereich der DS-RL, wenn das von den zuständigen Behörden (Polizei- oder Ordnungsbehörden) geführte Verfahren in ein konkretes Ordnungswidrigkeitenverfahren übergeht.

Dieses Verständnis hat der Bundesgesetzgeber im Rahmen der Anpassung des Datenschutzrechts an die DSGVO und die DS-RL durch das o. g. Datenschutz-Anpassungs- und -Umsetzungsgesetz EU zugrunde gelegt. Ausweislich der Gesetzesbegründung zu § 45 BDSG (BT-Drs. 18/11325, S. 110f.) sollen *„Datenverarbeitungen bei Verwaltungsbehörden wie z. B. Waffen-, Hygiene- oder Passbehörden, deren Aufgaben nicht mit den in § 45 genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den An-*

*wendungsbereich der Richtlinie und damit des Dritten Teils dieses Gesetzes fallen, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen“.*

Die Ermittlung, Verfolgung, Ahndung und Vollstreckung von Ordnungswidrigkeiten ist daher vom Anwendungsbereich der DS-RL umfasst. Dadurch wird sichergestellt, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Im Interesse der Einheitlichkeit muss dies für alle Ordnungswidrigkeitenverfahren gelten und somit auch in Bezug auf die Datenverarbeitung durch Behörden, die nicht Polizeibehörden sind, soweit sie Ordnungswidrigkeiten verfolgen, ahnden und vollstrecken (s. auch Gesetzesbegründung zum DSAnpUG EU, BT-Drs. 18/11325, S. 110).

7. Für den Übergang vom Verwaltungsverfahren in das Ordnungswidrigkeitenverfahren ist darauf abzustellen, ob die jeweilige Behörde ihre Maßnahmen auf das Verwaltungsverfahrensgesetz oder das Gesetz über Ordnungswidrigkeiten (OWiG) stützt. Datenschutzrechtlich findet mit dem Übergang in das Ordnungswidrigkeitenverfahren die DS-RL und damit auch Teil 1 und 3 des Bundesdatenschutzgesetzes (BDSG 2018) bzw. das OWiG Anwendung.

Der damit verbundene Nachteil für die handelnden Ordnungs- und ggf. auch Polizeibehörden, dass ein datenschutzrechtlicher Regimewechsel zu beachten ist, lässt sich nicht vermeiden. Ein solcher Wechsel ist auch im Kontext anderer Rechtsgebiete nicht gänzlich unbekannt.