

Durchwahl

Telefon 0351/85471-120
Telefax 0351/85471-109

saechsdsb@
slt.sachsen.de*

Dresden,
22. Dezember 2020

Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten 2019

Berichtszeitraum: 1. Januar 2019 bis 31. Dezember 2019

Informationen zur Vorstellung des Tätigkeitsberichts

1. Inhalt des Tätigkeitsberichts

Der Tätigkeitsbericht enthält Einzelfälle aus der aufsichtlichen Praxis, gibt Hinweise zur Auslegung der Datenschutzvorschriften, bietet einen Überblick der Entschließungen, Beschlüsse, Orientierungshilfen und weitere Hinweise der Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder und zu in der Praxis bedeutenden gerichtlichen Entscheidungen im Berichtszeitraum.

Dem Tätigkeitsbericht vorangestellt ist ein Inhalts- und Abkürzungsverzeichnis und zum besseren Überblick zu den Themen- und Datenverarbeitungsbereichen ein Sachgebietsregister.

2. Tätigkeit und Arbeitsschwerpunkte im Überblick

Im letzten Berichtszeitraum war der Anteil der allgemeinen Beratungsanfragen etwas zurückgegangen. Demgegenüber hat sich der Anteil der Bearbeitungsvorgänge im Bereich der Europäischen Union und des internationalen Datenverkehrs verdoppelt.

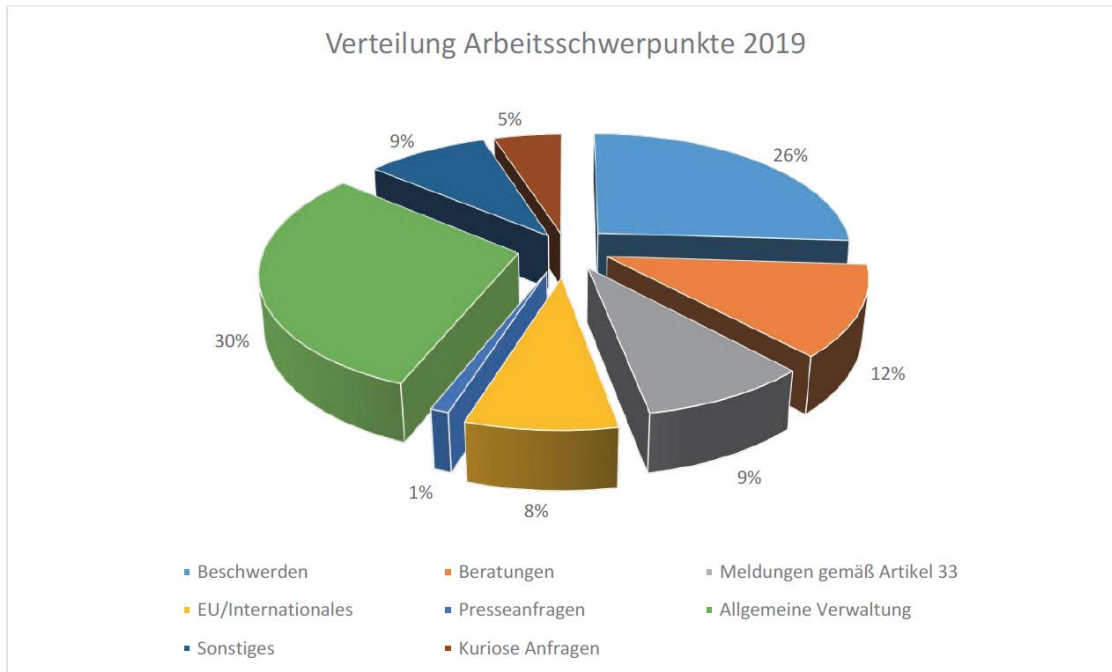
Bemerkenswert ist auch, dass der Anteil der Meldungen von Datenschutzverstößen gemäß Art. 33 Datenschutz-Grundverordnung nochmals um 67 % angestiegen ist, vergleiche Abschnitt **6.2.1** und den untenstehenden Überblick.

Hausanschrift:
Sächsischer
Datenschutzbeauftragter
Devrientstraße 5
01067 Dresden

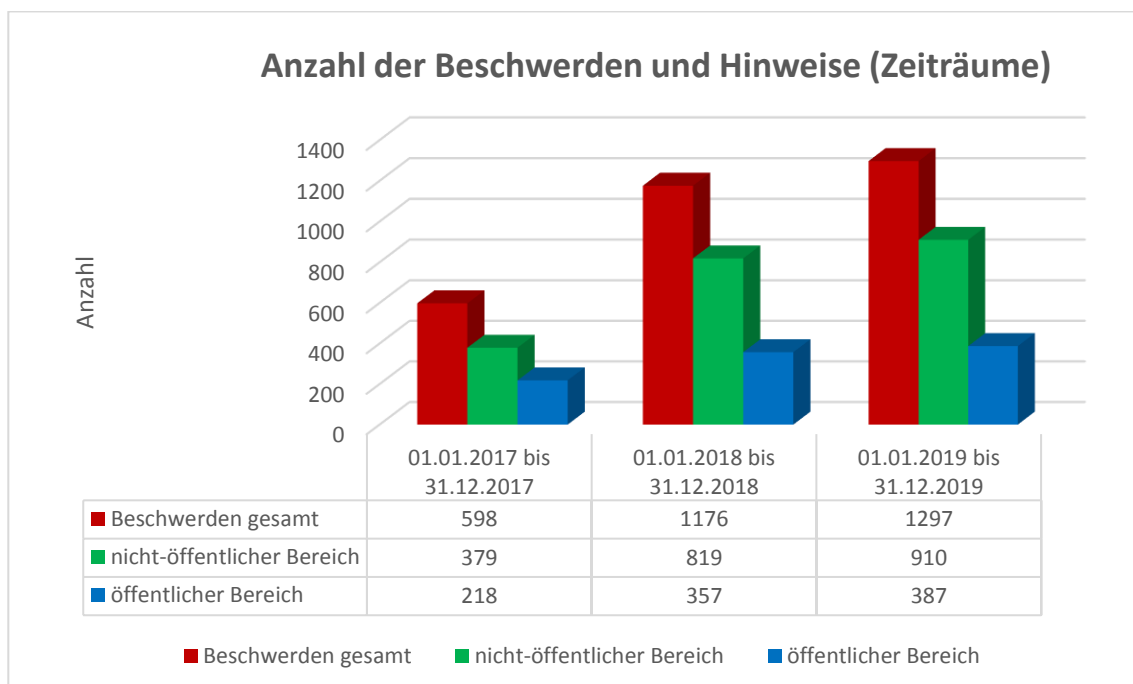
www.saechsdsb.de

Verkehrsanbindung:
Zu erreichen mit den Straßenbahnlinien 4 und 11
(Haltestelle Am Zwingerteich)

*Informationen über die Verarbeitung Ihrer personenbezogenen Daten gemäß Artikel 13 der Datenschutz-Grundverordnung und zum Zugang für verschlüsselte E-Mails finden Sie unter <https://www.saechsdsb.de/Datenschutzutzerklaerung>.



Die Fallmengen der Beschwerden stiegen auch im letzten Berichtszeitraum weiter an. 70 % der eingegangenen Beschwerden beziehen sich auf die Datenverarbeitung des nicht-öffentlichen Bereichs, d.h. auf die von Unternehmen, Vereinen, sonstigen Privatpersonen, vergleiche Abschnitt 6.2.2 und das nachfolgende Diagramm.



3. Themen und Einzelfälle des Berichtszeitraums

Beispielhaft wird auf nachstehende Inhalte des Tätigkeitsberichts hingewiesen:

Verfahrensvorschriften der Strafprozessordnung sind einzuhalten

Ein Tätigkeitsberichtsbeitrag befasst sich mit der Erhebung von Verkehrsdaten des Anschlusses eines Rechtsanwalts, vergleiche den **Abschnitt 8.6** dazu. Die Datenverarbeitung erfolgte vor dem Hintergrund einer umfangreichen Datenerhebung und Nutzung durch das Landeskriminalamt Sachsen als Polizeibehörde in einem strafrechtlichen Ermittlungsverfahren. Aufgrund seiner beruflichen Tätigkeit wurden die Kommunikationsdaten eines betroffenen Rechtsanwalts in vielen Bezügen und Ermittlungsverfahren erfasst und mit weiteren Datenbeständen abgeglichen. Nach Kenntniserlangung, dass es sich um einen Berufsgeheimnisträger handelte, dessen Daten nur eingeschränkt verarbeitet werden konnten, wurden die mehrere Jahreszeiträume betreffenden Informationen dennoch nicht vollständig gelöscht und die Benachrichtigung des Betroffenen erfolgte ebenso nicht vorschriftsgemäß.

Dabei kommt den Verfahrensvorschriften der Strafprozessordnung zum Schutz der besonderen Verhältnisse von Berufsgeheimnisträgern erhebliche datenschutzrechtliche Bedeutung zu. Die Strafverfolgungsbehörden und die sie unterstützenden Polizeibehörden sind pflichtig, die strafprozessualen Vorschriften einzuhalten. In dem Kontrollvorgang wurden seitens des Sächsischen Datenschutzbeauftragten das Landeskriminalamt und die Staatsanwaltschaft zur Einhaltung verbesserter Verfahrensabläufe und zur Sensibilisierung der Mitarbeiter angehalten.

Meldung von Datenschutzverletzungen

Die Vorschriften des Art. 33 Datenschutz-Grundverordnung verpflichten Verantwortliche bei einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden gegenüber der Datenschutzaufsichtsbehörde eine Meldung zu erteilen. Von einer Meldung kann nur abgesehen werden, soweit die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Die Anzahl der Meldungen hat im Berichtszeitraum des Jahres 2019 stark zugenommen und auf das Verfahren soll daher hier summarisch eingegangen werden. Es gingen etwa 450 dieser Anzeigen ein, vergleiche im einzelnen **Abschnitt 4.6**.

Am häufigsten handelt es sich um viel Versendung per Post, Telefax oder E-Mail und dabei nicht selten eine Verwechslung der empfangenden Personen. In diesen Fällen erhalten dritte Personen als nicht berechtigte Kenntnis von schützenswerten Inhalten. Diese betreffen zum Teil auch sensible Daten aus dem Gesundheits-, Versicherungs- und Bankenbereich.

Daneben bilden Einbruchs- und Diebstähle eine häufige Fallgruppe, bei denen Datenträger, Computer, Festplatten oder andere Speichermedien entwendet werden. Zumeist ist zu vermuten, dass es sich um Beschaffungskriminalität handelt, es den Tätern nicht vorrangig auf die Datenbestände, sondern auf werthaltige Hardware, wie Computer und Kameras ankommt. Dennoch ist auch in diesen Fällen eine damit verbundene Kenntniserlangung und Datenschutzverletzung durch unbefugte Dritte regelmäßig nicht auszuschließen. Auf die Datenbestände bezogene Verschlüsselungstechniken und Backups sowie der Verschluss bzw. die ordnungsgemäße Verwahrung der Datenträger sind aus technisch-organisatorischer Sicht notwendige Maßnahmen um Vorsorge zu treffen. Gehäuft aufgetreten sind auch Mängel der internen Datenspeicherung und -sicherung, Organisationsmängel, bei denen unter anderem unzulässige interne Zugriffe ermöglicht werden.

Trotz jahrelangen und etablierten E-Mail-Kommunikationsbetriebs werden immer noch offene E-Mail-Verteiler verwendet, bei denen die E-Mail-Kontaktdaten eines großen Adressatenkreises an sämtliche Empfänger – zumeist ungewollt – verbreitet werden.

Neben den sehr häufigen Meldungen treten auch Fälle von Cyberkriminalität, Handlungen und Straftaten, die durch die Nutzung von Kommunikations- und Informationstechniken begangen werden, auf. Zu nennen sind das Abgreifen personenbezogener Daten aus E-Mail-Postfächern und von Servern bzw. Online-Accounts.

Zur zukünftigen Fehlervermeidung sind regelmäßig erforderliche technisch-organisatorische Maßnahmen seitens der Verantwortlichen einzuleiten und mit der Datenverarbeitung betraute Personen sind, soweit erforderlich, zu sensibilisieren.

Zur durch den Verantwortlichen vorzunehmenden Risikoabschätzung enthält der Tätigkeitsbericht einen beispielhaften Beitrag unter **4.6.2**. Vergleiche auch den Beitrag mit den statistischen Informationen unter **6.2.6**.

Videografie

Zahlreiche Vorgänge und Fragen des letzten Berichtszeitraums betrafen wiederum den Bereich Videografie. Der Sächsische Datenschutzbeauftragte hat weiterhin in sehr großen Fallmengen Dashcam-Fälle im Rahmen von Ordnungswidrigkeitenverfahren zu bearbeiten, die nicht als Einzelfälle dargestellt worden sind.

Bei der behördlichen Beobachtung und Überwachung, vergleiche die Beiträge **2.2.16**, **8.2**, **8.4**, **8.6**, ist die vorgesehene Gesichtserkennung bei der sächsischen Polizei auf Grundlage von videotechnischen Verfahren hervorzuheben (Beitrag 8.2). Der Einsatz einer automatisierten Gesichtserkennung kann nur mittels Abgleich und daher unter Verwendung von großen Referenzdatenbankbeständen erfolgen. Aufgrund der noch nicht zureichenden technischen Reife und der möglichen Fehlerwirkung im Hinblick auf staatliche Eingriffsverwaltung betrachte ich diese Entwicklung in Gänze mit Sorge. Als besonders eingriffsintensiv ist auch der Einsatz von Videografie in Haftzellen anzusehen, vergleiche den Beitrag unter **8.4**. Was die strukturierte Überwachung mittels Videografie betrifft, zeigt der Bericht zu der Videoüberwachung im Chemnitzer Innenstadtbereich auf, welche grundrechtlichen Effekte am Beispiel des Versammlungsrechts mit einer weitergehenden Flächen weiten Videoüberwachung einhergehen können, vergleiche den Beitrag unter 8.6.

Grundlegende Überlegungen zur Videografie enthält auch der Beitrag **2.2.16**, der die Umstände im Zusammenhang mit dem im Berichtszeitraum stattgefundenen Einbruch im Grünen Gewölbe skizziert.

Der Beitrag unter **2.2.2** befasst sich mit der interessanten Frage der Befugnis von Privatpersonen, Video- und Bildbeweise mit Personenbezug für Behörden anzufertigen. Datenschutzrechtlich zuzugestehen sind derartige Anzeigehandlungen grundsätzlich lediglich selbst betroffenen Personen. Von großer praktischer Bedeutung sind die Überlegungen zur rechtlichen Zulässigkeit von Videoüberwachung in Fahrstuhlanlagen, **2.2.15**. Einen Überblick über die weitreichenden Informationspflichten bei Videografie bietet der Beitrag unter **3.1.1**.

Hinzuweisen ist auf die Informationsmaterialien der Datenschutzkonferenz unter **7.3**, Ziffer 6 bis 9 und auf die vielen Ordnungswidrigkeitenverfahren in dem Bereich, dargestellt unter **6.4.1**.

4. Ausblick und Aktuelles

Vorsitz der Datenschutzkonferenz

Im laufenden Jahr – 2020 – hatte der Sächsische Datenschutzbeauftragte den turnusmäßigen Vorsitz der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder inne. Auch ein Jubiläum, die 100. Datenschutzkonferenz, war durchzuführen. Die entscheidenden Konferenzen und Sitzungen konnten pandemiebedingt nur per Videokonferenz durchgeführt werden, was die Abläufe erschwerte. Der Vorsitz konnte gleichwohl erfolgreich bewerkstelligt werden. Die Konferenz befasste sich in der Amtszeit des Sächsischen Datenschutzbeauftragten mit entscheidenden Angelegenheiten und grundlegenden Problemen, u. a. mit der Frage des datenschutzkonformen Einsatzes von Windows 10, mit der Initiative der Exekutive zur Aufweichung von Ende-zu-Ende-Verschlüsselungen zugunsten von Sicherheitsbehörden und Nachrichtendiensten, mit der gesetzgeberischen Ausgestaltung der Telekommunikations-Bestandsdatenauskunft sowie mit der in Deutschland noch immer ausstehenden Umsetzung der „ePrivacy“-Richtlinie (RL 2002/58/EG). Einzelheiten sind auf der Internetpräsenz unter www.datenschutzkonferenz-online.de abrufbar.

Hinzuweisen ist auf die letzte Amtshandlung des Sächsischen Datenschutzbeauftragten als Vorsitzendem der Konferenz, die Durchführung des Europäischen Datenschutztags 2021 mit dem Thema „Transborder transfers - Herausforderungen des internationalen Datentransfers aus Sicht der Datenschutzkonvention 108+ und der DSGVO“. Die Veranstaltung wird am 28. Januar 2021 von 13:00 Uhr bis 16:30 Uhr als Online-Veranstaltung durchgeführt (. Eine Anmeldung ist bis zum 15. Januar 2021 auf der Internetseite des Bundesministeriums des Innern, für Bau und Heimat unter www.bmi.bund.de/convention108 möglich. Hier finden sich auch der Veranstaltungsablauf und weitere Informationen.

Pandemiebekämpfung in Sachsen

Aktuell kommt es zu zahlreichen Nachfragen und Beschwerden betroffener Personen und Verantwortlicher – datenverarbeitende Stellen – bezogen auf behördliche Maßnahmen und/oder Datenverarbeitungen von nicht-öffentlichen Stellen zur Bewältigung der aktuellen Pandemie bzw. zur Umsetzung der aktualisierten Corona-Schutz-Verordnung. Große rechtliche Unsicherheit besteht in der Praxis unter anderem, was die Frage des

Inhalts eines Attestes und das Verfahren zur Befreiung von der Mund- und Nasenschutzpflicht angeht. Der Sächsische Datenschutzbeauftragte hat hierzu Hinweise erteilt:

- Dem ärztlichen Zeugnis muss zu entnehmen sein, für welche Person die Befreiung ausgestellt wurde.
- Die Diagnose bzw. Begründung, aus welchen gesundheitlichen Gründen keine Mund-Nasenbedeckung getragen werden kann, muss nach Auffassung des für Gesundheitsfragen zuständigen Sächsischen Staatsministeriums, mit der ich übereinstimme, nicht angegeben sein. Betroffene Personen sollten bei der Ausstellung des Attestes darauf achten, dass die ärztlichen Nachweise keine Diagnoseinformation, sondern allein die Tatsache, dass der Mund- und Nasenschutz aus medizinischen Gründen enthalten.
- Des Weiteren muss der Arztstempel auf dem ärztlichen Zeugnis ersichtlich und lesbar sein.
- Abgesehen von Kinderbetreuungs- und Schuleinrichtungen, bei denen Ablichtungen der Atteste sind die Atteste nicht zu kopieren. Zur Glaubhaftmachung ist nach der geltenden Verordnung die lediglich die Einsichtnahme zu gewähren.

Die vollständigen Hinweise zu der Frage sind unter

https://www.saechsdsb.de/images/stories/sdb_inhalt/oeb/Information_Mund-Nasen-Schutz.pdf auf der Seite des Sächsischen Datenschutzbeauftragten abrufbar und nachzulesen.

Unter <https://www.saechsdsb.de/corona-pandemie> finden sich zudem weitere Empfehlungen, Hinweise und Musterformulare zur zulässigen Datenverarbeitung, unter anderem im Arbeitsverhältnis, beim Home-Office und zur Kontaktdatenerhebung.

Stellensituation

Zum Abschluss des Berichtszeitraums war der seitens des Haushaltsgesetzgebers trotz der nach Wirksamwerden der Datenschutz-Grundverordnung absehbaren neuen Aufgaben nur verzögert zugestandene Stellenaufwuchs auf 31 Vollzeitstellen noch nicht umgesetzt. In Anbetracht der aufgrund der Pandemie eingetretenen Verschlechterung der öffentlichen Haushaltslage wird seitens des Sächsischen Datenschutzbeauftragten der stetig geforderte zureichende Personalaufwuchs nun als schwer realisierbar einge-

schätzt. Nur wenige, aber nicht weitere Stellen in gemessen an den Aufgaben ausreichender Anzahl, sollen der Datenschutzaufsichtsbehörde nach Vorstellung der Regierung noch zugestanden werden. Eine noch nicht adäquate Stellenausstattung der Behörde führt zu verlängerten Zeiten beim Abschluss und ermöglicht bei hohem Geschäftsanfall zwangsläufig häufig keine tiefere Bearbeitung der Vorgänge.