

Sie wurden bei der Kommunalwahl in den Kreistag des Kreises Stormarn gewählt. Herzlichen Glückwunsch dazu.

Ihre Rechte und Pflichten ergeben sich hauptsächlich aus

- der Gemeindeordnung des Landes Schleswig-Holstein (GO),
- der Geschäftsordnung, die sich das Gremium gibt,
- der Landesverfassung des Landes Schleswig-Holstein und verfassungsrechtlichen Garantien.

Als ehrenamtlich tätige Bürgerin oder Bürger unterliegen Sie – auch über die Beendigung Ihrer Tätigkeit hinaus – einer Verschwiegenheitspflicht nach § 21 Abs. 2 GO.

Im Rahmen Ihrer Tätigkeit haben Sie Zugang zu personenbezogenen Daten. Beispiele sind:

- Personalangelegenheiten
- Baugenehmigungen und sonstige Planungsvorhaben
- Grundstücksangelegenheiten
- Vergabe
- Spenden

Daher sind Sie auch für die Einhaltung datenschutzrechtlicher Vorgaben verantwortlich.

Das Datenschutzrecht ändert sich durch die ab dem 25. Mai 2018 geltende EU Datenschutzgrundverordnung (DSGVO) wesentlich. Dieses Merkblatt gibt Ihnen einen Überblick.

Gibt es ein Recht auf Datenschutz?

Das Recht auf informationelle Selbstbestimmung wird hergeleitet aus Art. 2 (1) i.V.m. Art 1 (1) des Grundgesetzes (Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten).

Datenschutz ist zudem als Grundrecht in Artikel 8 der EU Grundrechte Charta verankert: *Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*

Was sind personenbezogene Daten?

"personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person, identifiziert werden kann.

Was ist Datenverarbeitung?

"Verarbeitung" bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Was ist nicht automatisierte Verarbeitung?

Nicht automatisierte Verfahren sind Verfahren, die sich keiner IT bedienen, also Daten in Papierform.

Welche Risiken können aus einer Verarbeitung personenbezogener Daten entstehen?

Beispiele hierfür werden im Erwägungsgrund 75 der DSGVO genannt, die Liste ist nicht abschließend:

- physischer, materieller oder immaterieller Schaden, bis hin zu Gefahr für Leib und Leben
- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanziellen Verlust,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten (Daten von Ärzten, Steuerberatern, Anwälten),
- andere erheblichen wirtschaftlichen oder gesellschaftlichen Nachteile
 - wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren,
 - wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen betreffende Daten verarbeitet werden,
 - wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen,
 - wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder
 - wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Wer ist Verantwortlicher?

"Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

Die meisten Daten, die Sie zur Ausübung Ihres Mandates benötigen, werden in der Verwaltung verarbeitet und Ihnen von der Verwaltung zur Verfügung gestellt. Damit ist zunächst einmal die Verwaltung Verantwortlicher im Sinne des Datenschutzes.

Da Sie nicht Teil der Verwaltung sind, unterliegen Sie keinerlei Weisungen durch die Verwaltung. Sobald die Daten Ihnen von der Verwaltung zur Ausübung Ihres Mandats zur Verfügung gestellt wurden und die Daten vollständig in Ihrer Verfügungsgewalt sind (Mitnahme von Akten in Papierform, Herunterladen von Daten aus einem Ratsinformationssystem auf den eigenen PC usw.) sind Sie Verantwortlicher im Sinne des Datenschutzes und müssen die Einhaltung der Regelungen zum Datenschutz gewährleisten.

Gemeindevertretungen / Stadtvertretungen können in Ihrer Geschäftsordnung Regelungen zum Datenschutz definieren.

Wer ist Dritter? Dürfen Dritte Zugang zu personenbezogenen Daten haben?

„Dritter“ sind alle natürlichen oder juristischen Personen sowie Stellen, die nicht Betroffener, Verantwortlicher oder Auftragsverarbeiter im Sinne von Artikel 28 DSGVO sind. Zu Dritten

gehören auch Partner, Familienangehörige, Parteifreunde, Nachbarn, Freunde und Bekannte.

Dritte dürfen grundsätzlich keine personenbezogenen Daten erhalten, es sei denn, es gibt eine Rechtsgrundlage, die dies erlaubt oder fordert, oder eine Einwilligung der betroffenen Person.

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es gibt eine Ausnahmeregelung. Dies sind nach Artikel 6 Abs. 1 DSGVO:

- a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

In welchen Gesetzen ist der Datenschutz geregelt?

Zunächst ist erst einmal die EU Datenschutzgrundverordnung (DSGVO) anzuwenden. Die DSGVO enthält aber in einigen Bereichen Öffnungsklauseln, die nationale Regelungen zulassen. Dies betrifft z.B.

- die Datenverarbeitung im Beschäftigungsverhältnis (geregelt in Landesdatenschutzgesetz (LDSG) bzw. Landesbeamtengesetz (LBG))
- den Schutz von Sozialdaten (Sozialgesetzbücher (SGB), insbesondere SGB X)
- besondere Regelungen für Verarbeitungen in öffentlichen Stellen (LDSG)

Weitere Regelungen finden sich z.B. in spezifischen Gesetzen wie der Abgabeordnung (§ 30 AO – Steuergeheimnis), dem Meldegesetz, im Strafgesetzbuch (§ 203 StGB – Verrat von Privatgeheimnissen, auch bekannt als Berufsgeheimnis von Ärzten, Steuerberatern, Anwälten, Sozialarbeitern usw.) und vielen weiteren Gesetzen.

Für den Bereich Justiz und Inneres ist die Richtlinie EU 2016/680 „Justiz- und Inneres Richtlinie (JI-Richtlinie)“ anzuwenden. Sie wird in Schleswig-Holstein durch das Landesdatenschutzgesetz (ab Abschnitt 3) in nationales Recht umgesetzt und hat für Bußgeldstellen Relevanz.

Welche Grundsätze müssen bei der Verarbeitung personenbezogener Daten beachtet werden?

Grundsätze nach Artikel 5 Abs. 1 sind:

- Rechtmäßigkeit: Es muss eine zulässige Rechtsgrundlage für die Verarbeitung geben.
- Verarbeitung nach Treu und Glauben

- **Transparenz:** Die betroffene Person soll wissen können, welche sie betreffenden personenbezogenen Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet wurden oder werden.
- **Zweckbindung:** Verarbeitung erfolgt nur für vorab festgelegte, eindeutige und legitime Zwecke.
- **Datenminimierung:** Die Daten und der Kreis der Zugriffsberechtigten werden auf das für die Zwecke der Verarbeitung absolut notwendige Maß beschränkt.
- **Richtigkeit:** Daten müssen richtig und aktuell sein. Daten, die im Hinblick auf die Verarbeitungszwecke unrichtig sind, müssen unverzüglich gelöscht oder berichtigt werden.
- **Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für die Zweckerfüllung notwendig ist.
- **Integrität und Vertraulichkeit:** Es müssen technische und organisatorische Maßnahmen getroffen werden, um eine angemessene Datensicherheit zu gewährleisten. Vertraulichkeit ist dabei der Schutz vor Verarbeitung durch Unbefugte, Integrität bedeutet, dass die Daten aktuell und unverfälscht sind. Ein weiteres in diesem Artikel genanntes Schutzziel ist die Verfügbarkeit – Daten sollen vor unbeabsichtigtem Verlust oder Zerstörung geschützt werden.

Wie müssen die Daten geschützt werden?

Es sollten angemessene technische und organisatorische Maßnahmen getroffen werden, um die in Artikel 5 Abs. 1 genannten Ziele zu erfüllen. Einige mögliche Maßnahmen sind:

- Schutz von Papierunterlagen und Bildschirmen gegen unberechtigte Einsichtnahme
- Verwahren Papier in verschlossenen Schränken
- Sichere Vernichtung von Papier (Aktenvernichter mit Stufe P4/P5 nach DIN 66399) und Datenträgern (Festplatten, USB-Sticks, Smartphones)
- Mithören von Gesprächen und Telefonaten vermeiden
- Keine Übertragung vertraulicher Informationen in unverschlüsselten E-Mails
- Datensicherung
- Verschlüsselung mobiler Datenträger
- Aktueller Virens Scanner und Firewall
- Keine Nutzung der für die Mandatsarbeit genutzten PCs und Smartphones durch Dritte (auch nicht durch Familienangehörige)
- keine Weitergabe von Informationen an Dritte, wenn es keine Rechtsgrundlage gibt

Was ist mit Rechenschaftspflicht gemeint?

Der Verantwortliche muss nicht nur die Regelungen zum Datenschutz einhalten, sondern er muss durch geeignete Dokumentationen und Durchführung von Soll- / Ist-Vergleichen auch die Einhaltung nachweisen können.

Was ist bei Datenschutzpannen zu tun?

Bei Verletzungen des Schutzes personenbezogener Daten sind die Ursachen zu klären, Auswirkungen zu untersuchen und Abhilfe zu schaffen. All dies muss dokumentiert werden (Artikel 33 Abs. 5 DSGVO) und auf Verlangen der Datenschutzaufsichtsbehörde zur Verfügung gestellt werden.

Wenn die Verletzung des Schutzes personenbezogener Daten vermutlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen könnte, ist die Datenschutzaufsichtsbehörde (ULD in Kiel) binnen 72 Stunden vom Verantwortlichen zu informieren (Artikel 33 DSGVO).

Wenn der Vorfall vermutlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen könnte, sind auch alle Betroffenen unverzüglich zu informieren. Dies ist insbesondere dann der Fall, wenn folgende Datenarten betroffen sind:

- Gesundheitsdaten
- Bankdaten und Kreditkarteninformationen
- Sozialdaten
- Personaldaten (hierzu gehören auch Bewerberdaten)
- Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (z.B. Steuergeheimnis)
- Biometrische oder genetische Daten
- Daten über rassische und ethnische Herkunft
- politische Meinungen, religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Daten zum Sexualleben oder der sexuellen Orientierung
- Daten über strafrechtliche Verurteilungen und Straftaten

Welche Rechte haben die betroffenen Personen?

Die Rechte der betroffenen Personen sind in den Artikeln 12 bis 23 und 82 DS-GVO geregelt.

- Ersatz für materielle und immaterielle Schäden, die aus Verstößen gegen die DS-GVO entstanden sind. Dabei kann sich die betroffene Person auch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht,... deren satzungsmäßige Ziele im öffentlichem Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig ist, vertreten lassen, wie z.B. Gewerkschaften, Verbraucherzentrale, und andere (Klagerecht der Verbände).
- Transparente Information und Kommunikation, Antworten auf Anfragen zu Betroffenenrechten innerhalb eines Monats, in Ausnahmefällen Verlängerung möglich
- Informationen bei Datenerhebung
- Auskunftsrechte
- Recht auf Berichtigung
- Recht auf Löschen bzw. Recht auf Vergessen werden
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht
- Beschwerderecht bei der Aufsichtsbehörde

Wer ist die zuständige Datenschutzaufsichtsbehörde?

ULD – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Holstenstraße 98
24103 Kiel

mail@datenschutzzentrum.de

Telefon: 0431 988-1200
Fax: 0431 988-1223