Deutsche Lebens-Rettungs-Gesellschaft

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)

Als Funktionsträger:in (alle sich ehrenamtlich im DLRG Landesverband Hessen e.V. – DLRG Hessen – engagierenden Mitglieder) besteht Zugriff auf vertrauliche und personenbezogene Daten.

Die DLRG Hessen möchte diese Daten schützen. Aus diesem Grund ist die DLRG Hessen darauf bedacht, alle Funktionsträger:innen darüber in Kenntnis zu setzen, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten (erheben, speichern, verändern, nutzen, weitergeben, etc.). Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine andere gesetzliche Regelung die Verarbeitung erlaubt oder eine Verarbeitung dieser Daten vorgeschrieben ist. Außerdem müssen diese Daten vertraulich behandelt und dürfen Dritten nicht zugänglich gemacht werden. Genaue Hinweise dazu können im Artikel 5 Abs. 1 DSGVO nachgelesen werden.

Aus den Regelungen des Artikel 5 DSGVO leiten wir für die DLRG Hessen einige Hinweise für die mobile Arbeit und die Nutzung von eigener Hardware ab und bitten, diese zu beachten:

1) Alle Funktionsträger:innen sind für den für die Aufgabenerledigung geeigneten Arbeitsplatz selbst verantwortlich und tragen die Kosten für Internet und Virenschutz.
2) Alle Funktionsträger:innen statten eigene Geräte vor Benutzung mit nötigen Sicherheitsvorkehrungen wie z.B. einem guten Passwort aus und nutzen dieses auch. Im Falle der Nutzung von mobilen Endgeräten sind Betriebs- bzw. Sicherheitsupdates möglichst früh durchzuführen.
3) Passwörter sollten eine Mindestlänge von 10 Stellen haben (bei Smartphones mindestens einen 4-stelligen PIN) und Groß- und Kleinschreibung, Zahlen und Sonderzeichen verwenden. Passworte dürfen nicht an Dritte weitergegeben werden. Wer eine 2-Faktor-Authentifizierung (z.B. zusätzliche Authentifizierung mit Fingerabdruck oder eine Authentificator-App) nutzen kann, wird gebeten, dies auch zu tun.
4) Mobile Datenträger können leicht unterwegs verloren gehen oder gestohlen werden. Daher sollten vertrauliche Informationen auf mobilen Datenträgern mit geeigneter Software verschlüsselt werden. Oft ist dies schon über Bordmittel z.B. bei Windows verfügbar.
5) Es sollten möglichst keine fremden mobilen Datenträger (z.B. USB-Sticks) in Laptops eingeführt werden, da es hierüber zur Verbreitung von Malware kommen kann – gerade wenn z.B. der USB-Stick oft in anderen Geräten verwendet wird.
6) DLRG-Daten und Unterlagen sind bei der mobilen Arbeit so zu schützen, dass Dritte - insbesondere auch im Haushalt lebende Personen - keine Einsicht und/oder keinen Zugriff nehmen können. Außerdem ist Stillschweigen zu wahren über die Inhalte, mit denen Funktionsträger:innen im Rahmen der Arbeit bei der DLRG in Verbindung kommt.

Deutsche Lebens-Rettungs-Gesellschaft

7) DLRG-E-Mails dürfen nicht an private E-Mail-Konten weitergeleitet werden. Es werden persönliche DLRG-E-Mail-Adressen für alle Funktionsträger:innen eingerichtet, die entweder über den DLRG-Webmailer oder über Einbindung einer eigenen Software (z.B. Outlook) abgerufen und verwaltet werden können.
8) Dokumente, im speziellen E-Mail-Anhänge, die personenbezogene oder andere sensible Daten beinhalten, sollten per E-Mail außerhalb des DLRG-Netzwerks nur verschlüsselt oder mit einem Passwort belegt versandt werden.
9) E-Mail-Anhänge, im speziellen Office-Dateien, bergen Gefahren. Beim Öffnen dieser Dateien, wird man aufgefordert, die Bearbeitungsfunktion zu aktivieren. Dadurch wird das Ausführen von Makros erlaubt und mögliche Malware, die in den Dateien inkludiert wurde, können großen Schaden auf dem Rechner anrichten. E-Mail-Anhänge sind daher grundsätzlich vor dem Öffnen zu prüfen bzw. die Absende-Adresse zu verifizieren. Die Betreffe dieser E-Mails sind ebenfalls unter genauen Augenschein zu nehmen. Verdächtige E-Mails sind besser direkt zu löschen.
10) Die Nutzung von WhatsApp ist aus unterschiedlichen Gründen nicht DSGVO-konform. Eigentlich müsste von allen Personen des eigenen Adressbuchs eine Einwilligung für die persönliche Nutzung dieses Dienstes bzw. für die Nutzung vieler Dienste des Meta-Konzerns eingeholt werden. Da sich dies kaum umsetzen lässt, empfehlen wir, DSGVO-konforme Alternativen wie „Threema“ oder „Signal“ zu nutzen und auch ganze Gruppen dazu aufzufordern.
11) Ab der Bereitstellung der MS 365-Funktionen wird bis zu einem noch näher zu benennenden Stichtag die Nutzung von Speichern außerhalb der von der DLRG betriebenen Speichermöglichkeiten / Clouds untersagt. Näheres hierzu regelt ein Rundschreiben, aus dem die Übergangszeiträume hervorgehen.
12) Die von der DLRG an Funktionsträger:innen überlassene Arbeitsmittel sind nach Ausscheiden aus der Funktion zurückzugeben.
13) Alle Funktionsträger:innen haben die Möglichkeit, jährlich an einer Datenschutzschulung im E-Learning-Format teilzunehmen, sofern nicht in regelmäßigen Abständen eine Schulung z.B. beim Arbeitgebenden absolviert wird. Dieses Angebot ist eigenverantwortlich wahrzunehmen.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Die Zustimmung zu dieser Erklärung erfolgt elektronisch. Alle Funktionsträger:innen erhalten dazu den Bestätigungslink per E-Mail.