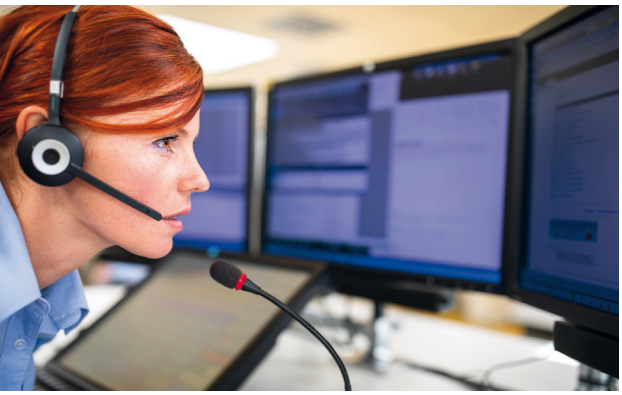
Notfallmanagement trifft auf Datenschutz: Eine unmögliche Beziehung?

Datenschutz im Rahmen der Katastrophenvorsorge



©lightpoet – stock.adobe.com

Entgegen landläufiger Meinung ist Datenschutz kein Hemmnis, wenn es um Krisenbewältigung geht. Die Datenschutzgrundverordnung (DSGVO) liefert sogar einen Erlaubnistatbestand, welcher den Datenschutz in den Status des Ermöglichers einer funktionierenden Geschäftsfortführungsplanung erhebt. Eine enge Verzahnung von Notfallmanagement und Datenschutz durch rechtmäßige Nutzung einer gemeinsamen Datenbasis birgt großes Potenzial.

Von Daniel Linder, HiScout GmbH

Corona Pandemie: Lockdown. Flutkatastrophe im Ahrtal: Zusammenbruch der Kommunikationsinfrastruktur. Energiekrise: Blackout. Und was kommt dann?

Seit der Corona-Pandemie ist Business-Continuity-Management (BCM) in den Fokus vieler Organisationen gerückt. Darin beinhaltete notwendige Maßnahmen stoßen häufig frontal mit Herausforderungen zusammen, die mit der Aussage „Unmöglichkeit wegen Datenschutz" gut zusammengefasst werden können. Wenn dieses Argument auftaucht, ist aber häufig nicht der Datenschutz das eigentliche Problem. Viel eher ist es die ungenaue Kenntnis der im Datenschutz herrschenden Vorschriften oder die diffuse Angst, ein Bußgeld aufgrund von Fehlern im Umgang mit personenbezogenen Daten auszulösen. Dass guter Datenschutz selten ein Hemmnis für das „ob", sondern eher ein Treiber des „wie" ist, ist an folgendem Fallbeispiel gut erkennbar.

Beispiel: Kommunikation im Krisenfall

Eine Organisation hat eine Software eingeführt, mit der Beschäftigte per Push-Nachricht auf ihrem Mobiltelefon kontaktiert werden können. Dies soll im Notfall eine schnelle und flächendeckende Kommunikation an die Belegschaft ermöglichen. So soll zum Beispiel im Katastrophenfall durch einen ersten, direkten Kontaktversuch zu den vermutlich betroffenen Mitarbeitenden schnell Klarheit erlangt werden, ob Personal der Organisation von der Katastrophe betroffen ist oder ob es gar Vermissten- oder Todesfälle gibt.

Um im Krisenfall einen zweiten, erweiterten Versuch der Kommunikationsaufnahme starten zu können, wird erwägt, vorsorglich weitere Ansprechpartner aus dem nahen Umfeld der eigentlich zu erreichenden Personen in die Rufliste aufzunehmen. Bei einem Personenschaden oder dem Verlust des persönlichen Kommunikationsmediums könnte so noch eine Verbindung hergestellt werden. In unserer Beispielorganisation hat der agierende Datenschutzbeauftragte (DSB) jedoch Bedenken, dass hier personenbezogene Daten unrechtmäßig erhoben und verarbeitet würden. Er rät dem Verantwortlichen daher dringend davon ab, Daten zu erheben, die nicht direkt der angestellten Person zuzuordnen sind. Die Aufnahme der Daten des erweiterten Kreises von Kontaktpersonen unterbleibt in der Folge.

Die Beispielorganisation besitzt Arbeitsstätten und Personal in einem Überflutungsgebiet. Als es zu einer Flutkatastrophe kommt, versucht die benannte Beispielorganisation Klarheit darüber zu erlangen, ob und wie viele Angestellte von der Katastrophe betroffen sind. In der ersten Runde der Kontaktaufnahme melden sich rund 30 Personen nicht mit einer Entwarnung oder einem Hilfeersuchen zurück. Es ist zu befürchten, dass diese Personen ein Opfer der Flut geworden sind. Nach einem angemessenen Zeitraum wird eine zweite Nachricht an diese Personengruppe versandt. Auf diese Meldung antworten 25 weitere Personen, die aus den verschiedensten Gründen von der ersten Nachricht nicht erreicht wurden. Fünf Personen, die auch alle zum Katastrophenzeitpunkt im Katastrophengebiet verortet werden, sind weiter unauffindbar.

Die nun einsetzende Suche gestaltet sich kostspielig, langwierig und schwierig. Am Ende stellt sich heraus, dass alle fünf gesuchten Angestellten wohlauf sind, sich

aber aus verschiedenen Gründen nicht melden konnten: Verlust des für den Empfang der Meldung notwendigen Mobilgerätes, Verlust der Energieversorgung, um das Gerät zu laden, keine Zeit für nicht-überlebensnotwendige Handlungen und so weiter. Eine spätere Untersuchung des Ablaufs zeigt, dass es erreichbare Kommunikationsmöglichkeiten im nahen persönlichen Umfeld gegeben hätte. Wären also die Kontaktdaten aus dem Umfeld der Betroffenen vorhanden gewesen, hätte der Verbleib der Mitarbeitenden schnell aufgeklärt und eine nachhaltige Erreichbarkeit sichergestellt werden können.

Schlussfolgerungen

Folgende Überlegungen ergeben sich aus der Sicht des Datenschutzes, der als Hinderungsgrund für die Datenaufnahme angegeben wurde:

Zweck der Kontaktdatenverarbeitung ist, in einem Katastrophenfall (und auch nur dann!) den Verantwortlichen schnellstmöglich feststellen zu lassen, welcher der Angestellten eventuell in Not ist und Hilfe oder gar Rettung benötigt.

Ziele der Verarbeitung sind Interventionen im Interesse des Betroffenen, also finanzielle Hilfe, Beiträge zur körperlichen Unversehrtheit bis hin zu lebensrettenden Maßnahmen.

Die Erfassung und Verarbeitung der personenbezogenen Daten der Angestellten ist daher aus Gründen der gesetzlichen Fürsorgepflicht des Arbeitgebers oder aus vertraglicher Verpflichtung heraus möglich. Auch ein berechtigtes Interesse an der Unversehrtheit der „Human Resources" kann hier ganz klar angeführt werden. Als erste zu wählende Rechtsgrundlage ist aber Artikel 6 Abs. 1 lit. d DSGVO zu nennen: Die Verarbeitung zielt in unserem Beispiel zentral auf die Wahrung lebenswichtiger Interessen des Betroffenen ab.

Die Art der verarbeiteten Daten sind Kontaktdaten, genauer vermutlich Telefonnummer oder Messenger-Kennung sowie Name und Vorname. Die Rechtmäßigkeit der Verarbeitung kann daher ausschließlich auf Basis von Artikel 6 DSGVO hergeleitet werden, ohne dass die restriktiveren Rechtsgrundlagen aus Artikel 9 DSGVO eröffnet sind.

Zum Erfassen derselben Daten von weiteren kontaktierbaren Personen aus dem Umfeld der Angestellten müssen weitere Punkte in Betracht gezogen werden: Diese Daten können entweder auf der Basis einer Einwilligung der betroffenen Person oder auf Basis des berechtigten Interesses des Verantwortlichen verarbeitet werden. Auch hier sollte aber als erste zu betrachtende Rechtsgrundlage Artikel 6 Abs. 1 lit. d DSGVO ins Feld geführt werden. Dieser ermöglicht auch die Verarbeitung der Daten Dritter, sofern diese erforderlich sind, um lebenswichtige Interessen der Angestellten zu schützen.

Unabdingbar im Rahmen der Transparenzpflichten nach Artikel 14 DSGVO ist allerdings die Information der Dritten über die Verarbeitung ihrer Daten.

Ein weiterer Vorteil der Datenverarbeitung auf Basis des Schutzes lebenswichtiger Interessen anstelle der Verarbeitung auf Basis einer Einwilligung besteht im Wegfall der Freiwilligkeitsproblematik im Bereich von Angestelltenverhältnissen.

Ein zusätzliches Argument für die Ermöglichung der Verarbeitung sind angemessene technische und organisatorische Maßnahmen (TOM), die auf verschiedenste Art und Weise ausgestaltet werden können. Ein guter Einstieg kann eine komplette physische oder logische Sperrung der aufgenommenen Daten direkt nach der Aufnahme bis zur Verwendung im Ernstfall sein: Man kann die Kontaktdatensätze auf verschiedene Bruchteile aufteilen, sie verschlüsseln oder den Zugang über eine Multifaktor-/Multipersonen-Authentifizierung regeln, die erst im Krisenfall zugänglich wird. Die hier möglichen Schutzmaßnahmen sind vielfältig und tragen zu einer guten Argumentationsbasis für die geplante Verarbeitung bei, die den lebenswichtigen Interessen der Betroffenen dient.

Fazit

Gerade im Bereich des Katastrophenschutzes in der Geschäftsfortführungsplanung ist der Datenschutz aufgrund des Erlaubnistatbestands des Artikel 6 Abs. 1 lit. d DSGVO kein Hemmnis für eine Aufnahme und Verarbeitung von Daten, sondern ein Ermöglicher. In dieser Rolle hilft er, den Blick der Organisation für die notwendigen Maßnahmen zum Schutz und der Sicherung der krisenrelevanten Daten im Rahmen der verschiedenen Krisenbewältigungsprozesse zu schärfen. Wenn man einen gesicherten und strukturierten Umgang mit den Daten der Betroffenen voraussetzt, gibt es aus Sicht des Datenschutzes nur zwei Fragen zu klären: die Absicherung der Daten bis zu ihrem tatsächlichen Einsatz im Krisenfall sowie die Eintragung der Verarbeitungstätigkeit in das hierzu geführte Verzeichnis. Besonders wichtig ist hier die enge Verzahnung der beiden Fachbereiche Business-Continuity-Management und Datenschutz. Im Idealfall arbeiten beide Bereiche auf derselben Plattform und nutzen eine gemeinsame Datenbasis. Nur so kann sichergestellt werden, dass die Verarbeitung der personenbezogenen Daten im Krisenfall DSGVO-konform und den Ansprüchen des Krisenmanagements genügend vonstatten geht.