



Unabhängige Aufarbeitungskommission
für das Bistum Münster
Herrn Prof. Dr. Christian Schrapper
Krummer Timpen 63a
48135 Münster

Kaiserstraße 161
53113 Bonn

Postanschrift
Postfach 29 62
53019 Bonn

Tel.: 0228-103-290
Fax: 0228-103-299
E-Mail generalsekretaerin@dbk.de

AZ : PA S 0441/25

Bonn, den 28.05.2025

Ihr Schreiben vom 11.04.2025 im Kontext der Cyberangriffs auf die IT-Systeme der Deutschen Bischofskonferenz bzw. des VDD

Sehr geehrter Herr Prof. Schrapper,

zunächst einmal bitte ich um Entschuldigung für die verspätete Antwort auf Ihr o.g. Schreiben. Gerne beantworte ich dieses wie folgt:

Unmittelbar nach Bekanntwerden des Vorfalls am 11.02.2025 hat der VDD folgende Maßnahmen ergriffen:

- sofortige Isolierung der betroffenen Systeme
- Einschaltung externer IT-Sicherheitsspezialisten
- Zusammenarbeit mit den Datenschutz- und Strafverfolgungsbehörden
- umfassende Sicherheitsüberprüfungen und sofortige Maßnahmen zur Vermeidung zukünftiger Angriffe
- umgehende und fortlaufende Information der Öffentlichkeit und der Mitarbeitenden über den Sachstand

Der Angriff betraf die Deutsche Bischofskonferenz bzw. den Verband der Diözesen Deutschlands (VDD) insgesamt und richtete sich nicht gegen einzelne Organisationseinheiten oder auf bestimmte Datenbestände. Die Unabhängige Kommission für Anerkennungsleistungen (UKA) stand nicht im Fokus der Angreifer.

Zu Ihrer Frage nach der Verwahrung der Daten:

Zwar handelt es sich bei der UKA um eine unabhängige Kommission, jedoch verfügt sie nicht über eine eigene Rechtsträgerschaft. Organisatorisch ist sie an ihren Rechtsträger, den VDD, angebunden. Die von der UKA und ihrer Geschäftsstelle verarbeiteten Daten befanden sich auf den Servern der DBK bzw. des VDD als Rechtsträger der UKA. Sie sind jedoch ausschließlich für die Mitarbeitenden der Geschäftsstelle der UKA zugänglich. Selbstverständlich unterliegen die UKA-Daten umfassenden technischen und organisatorischen Schutzmaßnahmen – einschließlich regelmäßiger Datensicherungen (Backups).

Zu Ihrer Frage zum „Verbleib dieser abgeflossenen Daten“:

Die Analyse mit externen IT-Sicherheits- und Datenschutzexperten, ob und in welchem Umfang personenbezogene Daten durch den Cyberangriff betroffen sind, ist mittlerweile abgeschlossen. Trotz intensiver IT-forensischer Untersuchungen gibt es Stand heute keine Beweise für einen unrechtmäßigen Zugriff auf besonders schützenswerte Daten. Die Untersuchungen haben ergeben, dass weder im Darknet noch auf sonstigen Medienkanälen vertrauliche personenbezogene Daten aus unserer Organisation aufgetaucht sind. Insbesondere gibt es keinerlei Hinweise darauf, dass personenbezogene Daten von Betroffenen sexuellen Missbrauchs von dem Cyberangriff betroffen sind. Die Untersuchungen haben auch keine Anzeichen dafür ergeben, dass solche Daten kompromittiert oder veröffentlicht wurden.

Zu Ihren Fragen zur Arbeitsfähigkeit der UKA und ihrer Geschäftsstelle sowie zu den Bearbeitungszeiten der Anträge bei der UKA:

Bei der Geschäftsstelle der UKA war unmittelbar nach dem Cyberangriff nur eine telefonische Erreichbarkeit gegeben, jedoch war sie zeitnah nach dem Angriff wieder per E-Mail erreichbar. Ebenfalls zeitnah nach dem Angriff hat die UKA ihre Arbeit fortgesetzt; Anträge werden bearbeitet. Seit Ende März finden wieder Sitzungen statt. Die vollständige Arbeitsfähigkeit der UKA wird nach abgeschlossenem Aufbau der neuen IT-Infrastruktur gegeben sein. Gerade mit Blick auf eine Verkürzung der Bearbeitungszeiten wurde die Kommission durch zwei Neuberufungen auf 12 Mitglieder erweitert: Herr Rudyk und Frau Adams-Dolfen sind seit März bzw. Mai 2025 Mitglieder der Kommission. Diese Erweiterung erhöht die Arbeitskapazität der Kommission im Regelbetrieb. Die Kommission wird nach Wiederherstellung ihrer vollen Arbeitsfähigkeit die Bearbeitungszeiten bei der Sitzungsplanung berücksichtigen. Der Datenbestand der Geschäftsstelle der UKA wird in Kürze wieder vollständig zur Verfügung stehen.

Zu Ihrer Frage bzgl. der künftigen Datensicherung:

Wir arbeiten derzeit intensiv daran, die technischen und organisatorischen Maßnahmen zur Absicherung der Datenverarbeitung weiterzuentwickeln und auf einem hohen Sicherheitsniveau zu halten bzw. dieses auszubauen. Im Zuge der Wiederherstellung der Arbeitsfähigkeit der UKA sind verschiedene technisch-organisatorische Maßnahmen (TOM) geplant, um die Einhaltung insbesondere der Vorgaben aus weiterhin sicherzustellen (z.B. Netzsegmentierungen und stärkere Zugriffsbeschränkungen, evtl. eine Multi-Faktor-Authentifizierung, kontinuierliche Sicherheitsupdates, intensiviertes Monitoring der sicherheitsrelevanten Vorgänge, Schulung der Mitarbeitenden in Fragen der Informationssicherheit und des Datenschutzes). Diese Maßnahmen dienen nicht nur der kurzfristigen Wiederherstellung, sondern sind Teil einer langfristigen Strategie zur kontinuierlichen Verbesserung der Sicherheit und des Datenschutzes. Die Ergebnisse der mittlerweile abgeschlossenen forensischen Untersuchung sowie die Einschätzungen der Datenschutzaufsicht werden hierbei angemessene Berücksichtigung finden.

Zu Ihrer Frage der Information betroffener Personen über das Geschehene:

Von Beginn an haben wir in allgemeiner Form proaktiv über den Vorfall informiert: Über unsere Internetseite (vgl. unsere Pressemitteilungen vom 11.02., 27.02. und 30.04.2025) sowie im direkten Austausch mit relevanten Personengruppen – darunter dem Betroffenenbeirat bei der DBK und der UKA – haben wir fortlaufend und soweit es ermittlungstaktisch vertretbar war, über den Stand der Dinge berichtet.

Am 07.03.2025 wurde zudem ein spezielles Servicetelefon eingerichtet – insbesondere für Betroffene sexualisierter Gewalt, die einen Antrag bei der UKA gestellt haben. Allerdings verzeichnen wir nur sehr wenige telefonische Nachfragen und Mailanfragen (insgesamt im einstelligen Bereich) sowie wenige einzelne schriftliche Anfragen an das Sekretariat der Deutschen Bischofskonferenz. Aufgrund der geringen Nachfrage wurde die telefonische Erreichbarkeit der Servicestelle am 23.05.2025 eingestellt. Die E-Mail-Adresse servicestelle@dbk.de ist weiterhin erreichbar.

Die Frage, ob eine Benachrichtigung betroffener Personen nach § 34 KDG-VDD erforderlich ist, haben wir in jedem Stadium nach dem Cyberangriff sorgfältig geprüft; wir standen dabei in engem Austausch mit der zuständigen Datenschutzaufsicht. Eine Verpflichtung zur Benachrichtigung betroffener Personen besteht nach § 34 KDG-VDD dann, wenn die Verletzung personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen hat. Hätten gesicherte Erkenntnisse für eine Verletzung des Schutzes personenbezogener Daten vorgelegen und wären wir zu dem Ergebnis gekommen, dass ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen im Sinne des § 34 KDG besteht, hätten wir die involvierten Personen gemäß den gesetzlichen Vorgaben informiert. Da jedoch weder

identifizierbare Personen betroffen noch konkrete Schäden entstanden sind oder zu erwarten waren, lagen die Voraussetzungen für eine Benachrichtigungspflicht zu keinem Zeitpunkt vor, insbesondere nicht für die besonders vulnerablen Personengruppen.

Ich hoffe, Ihre Fragen mit diesen Ausführungen angemessen beantwortet zu haben. Für eventuelle Rückfragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen



Dr. Beate Gilles