Erfahrungsaustausch der betrieblichen Datenschutzbeauftragten

Joachimski
Datenschutzbeauftragter der
bayerischen (Erz-) Diözesen

Hauptthemen

- Die neueste Rechtsentwicklung
  - Das neue KDG
  - Die gerichtliche Verfahrensordnung
  - Was ändert sich in der Praxis?
- Kommunikation
  - per E-Mail
  - per Messenger
- Ergebnisse der Datenschutzaufsichtstätigkeit (Mayinger)
- Hinweise zur datenschutzgerechten Handhabung privater Konten bei sozialen Medien.

Europäische Union

- Die Europäische Union hatte bisher eine Datenschutzrichtlinie von 1995.
- Sie war nicht unmittelbar geltendes Recht, sondern verpflichtete nur die Mitgliedsstaaten, richtlinienkonformes Recht zu erlassen.
- Für Deutschland war das ohne Bedeutung, weil das deutsche Recht erheblich weiter ging als die Richtlinie.
- Die EU erließ aber 2016 schon eine Datenschutzverordnung, die am 25.5.2018 in Kraft treten soll. Sie ist dann unmittelbar geltendes Recht.
- In ihren Regelungen geht sie teilweise über das deutsche Recht hinaus, teilweise bleibt sie zurück.
- Die Gründe dafür: Immer mehr „Angreifer“ wollen – möglichst unerkannt – an die Daten der Bürger.

Facebook (What‘s App), Twitter, Google (Youtube)

Payback-Systeme oder Kundenkarten -Betreiber

„Legale“ Angreifer wie z.B. Preisausschreiben oder Antwort auf Werbebriefe

Schon vorhandene Vertragspartner des Kunden wie z.B. Kabelversorger, Telefonanbieter, Energieversorger

Alle wollen an meine Daten!

„Illegale“ Angreifer (Adresshandel, Phishing)

Warum wollen die Unternehmen eigentlich an die Daten der Bürger?

- Die Daten sind unmittelbar etwas wert: Ein Datensatz kann für (geschätzt) 0,60 € auf dem grauen Markt zu Werbezwecken verkauft werden.
- Für manche Unternehmen ist der Wert noch höher: Beispiel REWE-Payback. Mit diesem und ähnlichen Systemen wird eine ziemlich sichere Aussage darüber, *was Frau Mayer an einem Mittwochvormittag in ihrem örtlichen Laden kaufen wird,* ermöglicht und damit eine
  - wettbewerbssichere
  - kostengünstigere

  Lagerhaltung ermöglicht.

Datenschutzebenen bis 25.5.2018

Richtlinie

BDSG

Bundes- und teilweise Landesbehörden sowie nicht-öffentliche Stellen

Landesdaten-schutzgesetze

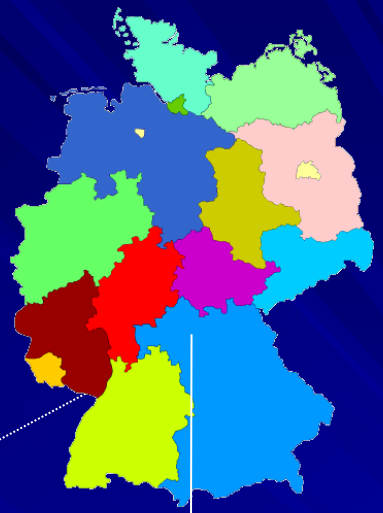
Landesbehörden

Art. 137 WRV

Kirchen

Die Rechtslage nach Inkrafttreten der VO 25.5.2018

Verordnung



BDSG nur, soweit in der VO vorbehalten

Art. 137 WRV, 140 GG

Behörden und nicht-öffentliche Stellen

Die Kirchen behalten ihr eigenes Datenschutzrecht

Datenschutzrecht der Kirchen

- Es besteht kirchliche Selbstverwaltungsfreiheit, Art. 137 WRV i.V.m. 140 GG
- Das BDSG ist in seinen Abschnitten 2 und 3 auf die Kirchen (auch bei privatrechtlichen Organisationsformen wie der Caritas) nicht direkt anwendbar.
- Die Kirchen behalten nach Art. 91 EU-VO ihre Datenschutz-Selbstverwaltung, sofern zum Zeitpunkt des Inkrafttretens am 25.5.2018 eine gleichwertige kirchliche Regelung vorliegt.
- Daran arbeiteten die zuständigen Gremien schon: Die KDO wird sich also noch ganz erheblich ändern.

EU-Datenschutz-Grundverordnung

- Nach Art. 91 diese Verordnung muss das kirchliche Datenschutzrecht mit demjenigen der Europäischen Union „in Einklang stehen“, d.h. es muss gleichwertig sein.
- Dies erfordert eine ganz erhebliche Anpassungsarbeit, welche sich gegenwärtig auf ihre letzte Phase hin zubewegt.
- Es liegt ein Entwurf der Arbeitsgruppe „Datenschutz und Melderecht“ vor, der noch ein letztes Mal von den kirchlichen Stellen diskutiert werden muss.

Wesentliche Änderungen im Hinblick auf den betrieblichen Datenschutzbeauftragten

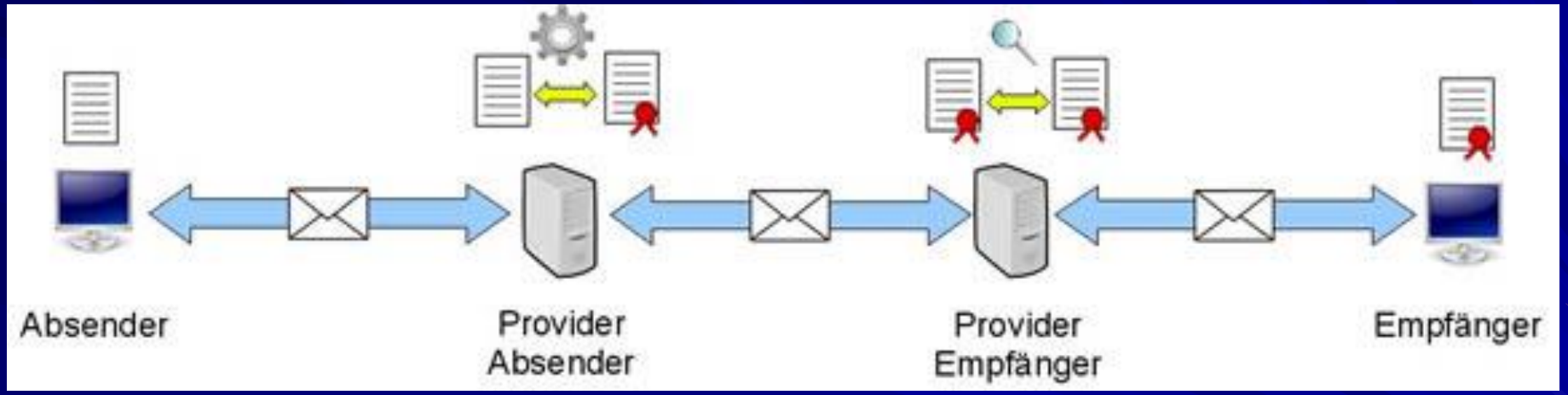
- In der verfassten Kirche wird sicher keine Mindestzahl der Beschäftigten mehr festgelegt, ab der ein betrieblicher Datenschutzbeauftragter vorhanden sein muss. Es muss ihn künftig immer geben.
- Festgeschrieben wird, dass der betriebliche Datenschutzbeauftragte „seine Dienststelle berät“. Eine Haftung lässt sich daraus nicht ableiten.
- Wer betrieblicher Datenschutzbeauftragter ist, muss bis zum 25. Mai 2018 dem Diözesandatenschutzbeauftragten mitgeteilt werden. Auch die Veröffentlichung des Namens zum Beispiel auf der Webseite wird zum Erfordernis.

Gerichtliche Überprüfung der Entscheidungen des Diözesandatenschutzbeauftragten

- Die EU-DS-GVO verlangt einen Rechtsweg gegen Entscheidungen des Diözesandatenschutzbeauftragten.
- Dieser findet sich nun im Entwurf einer Datenschutz-Gerichtsordnung.
- Das Datenschutzgericht wird beim VDD angesiedelt, bietet zwei Instanzen und hat seinen Sitz in Bonn.
- Die Ordensgemeinschaften sind teilnahmeberechtigt.
- Entscheidungen des Datenschutzgerichts binden dem Grunde nach die staatlichen Zivilgerichte in Fragen des Schadensersatzes.

Elektronische Kommunikation
Teil 1: E-Mails

- Wie sicher ist der E-Mail-Verkehr?



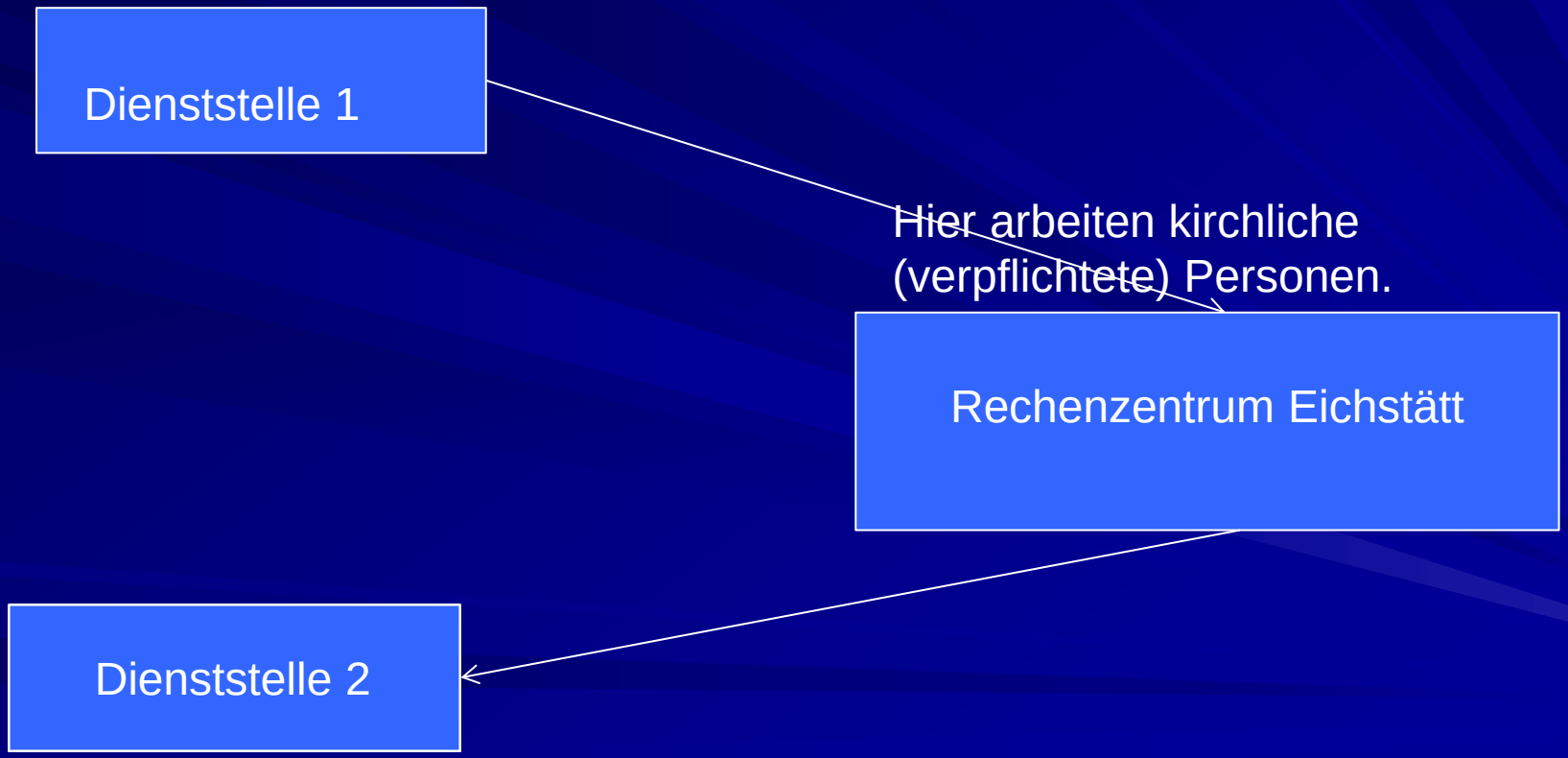
- Im Ergebnis kann an jedem Punkt die unberechtigte Kenntnisnahme erfolgen.
- Merksatz: Das normale E-Mail entspricht der Postkarte, nur das verschlüsselte dem Brief.

Wo können E-Mails unberechtigt mitgelesen werden?

- Zugriff auf Sender/ Empfängersystem
- Zugriff auf Mailserver, die zwischen Sender und Empfänger liegen
- Zugriff auf beliebige Netzwerkknoten (Router/ Switches) + unverschlüsselte Übertragung auf dem Streckenabschnitt
- Zugriff auf Netzwerkkabel + unverschlüsselte Übertragung zwischen Sender und Mailserver des Senders
- Zugriff auf Netzwerkkabel + unverschlüsselte Übertragung zwischen unterschiedlichen Mailservern
- Zugriff auf Netzwerkkabel + unverschlüsselte Übertragung zwischen Mailserver des Empfängers und Empfänger

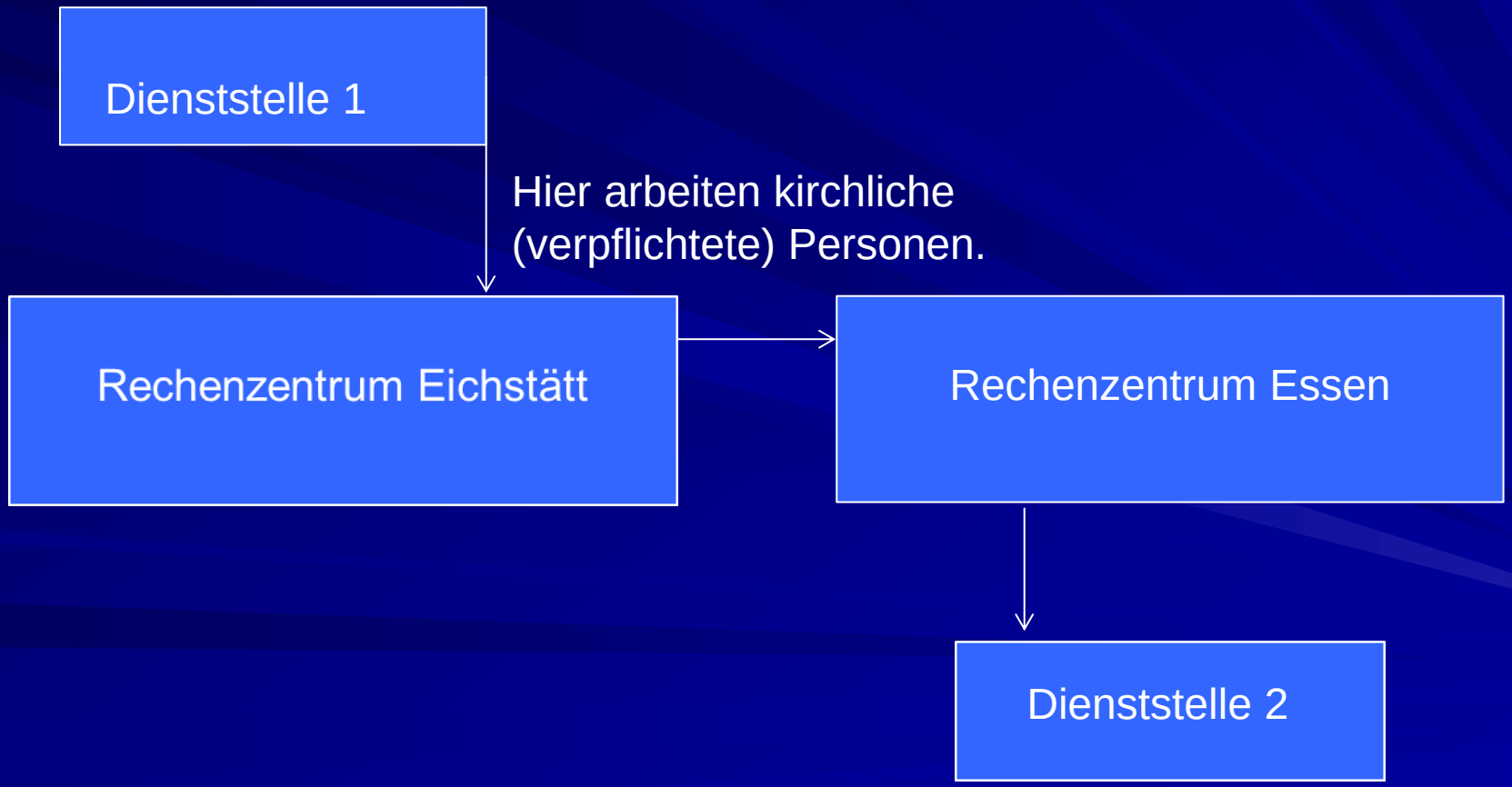
Gegenmaßnahmen und Sicherungen:

- Der E-Mail-Verkehr zwischen kirchlichen Dienststellen in Bayern ist sicher genug:



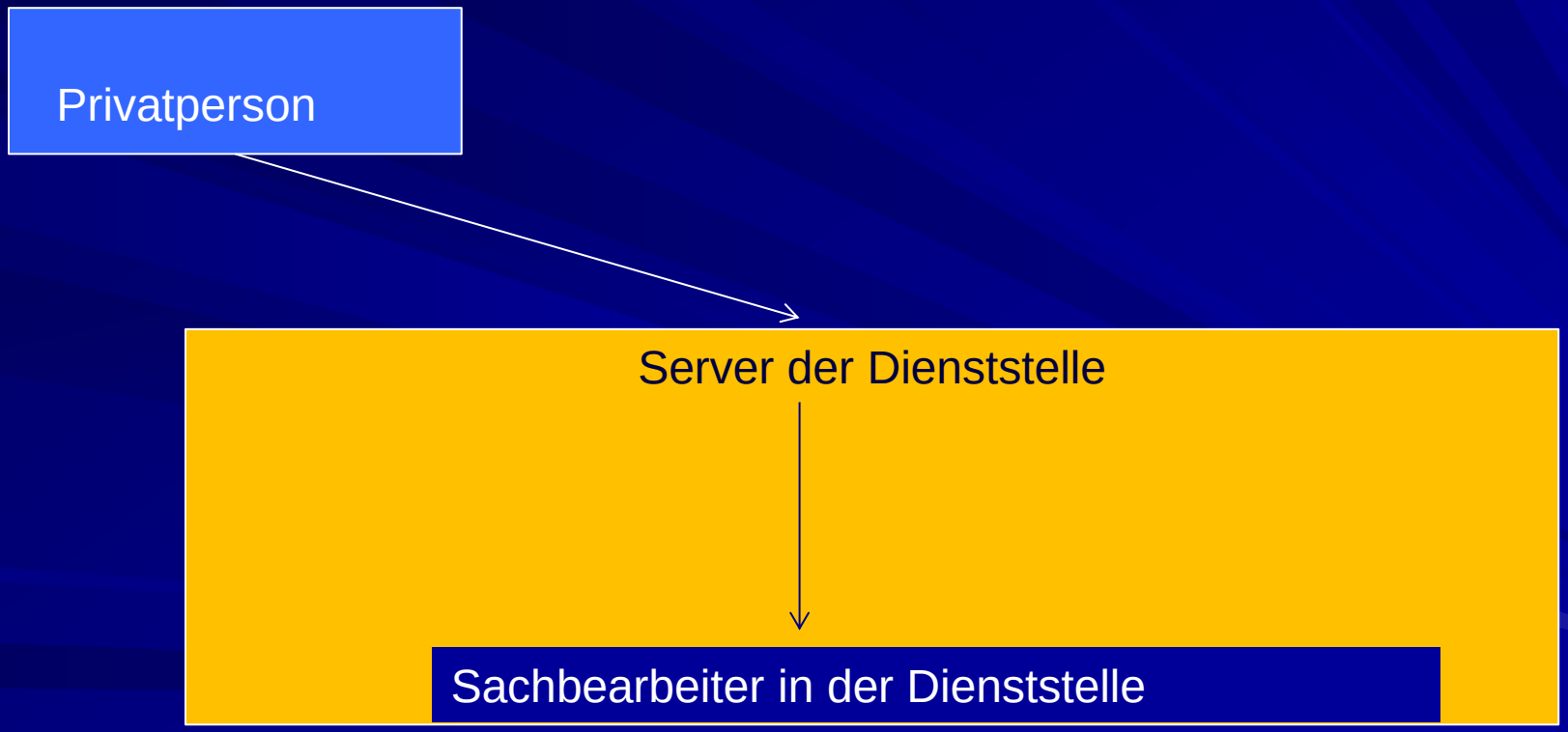
Gegenmaßnahmen und Sicherungen:

- Der E-Mail-Verkehr zwischen kirchlichen Dienststellen in Deutschland ist dann sicher genug, wenn nur kirchliche Rechenzentren eingeschaltet sind.



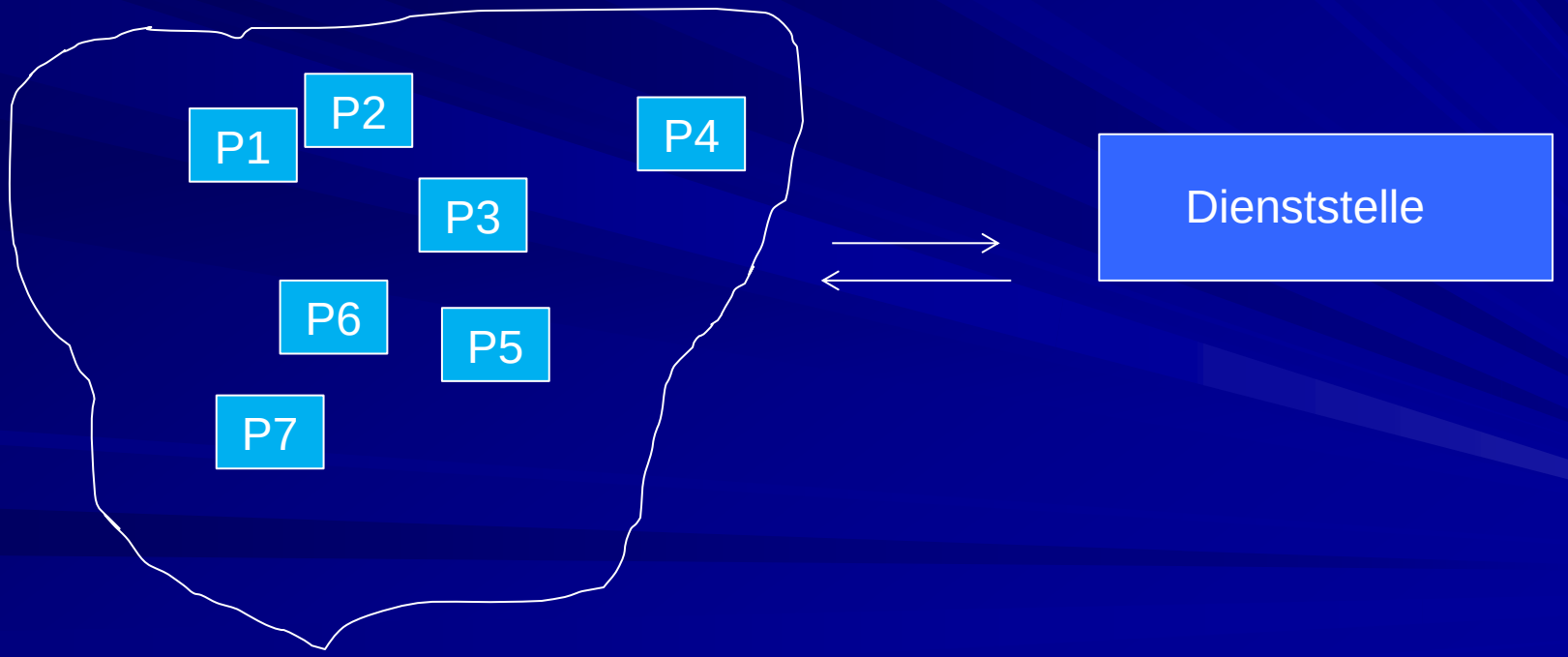
Gegenmaßnahmen und Sicherungen:

- Eine Privatperson kann sich direkt auf den Webserver einer Dienststelle einloggen und von dort ein E-Mail an den Sachbearbeiter verschicken:



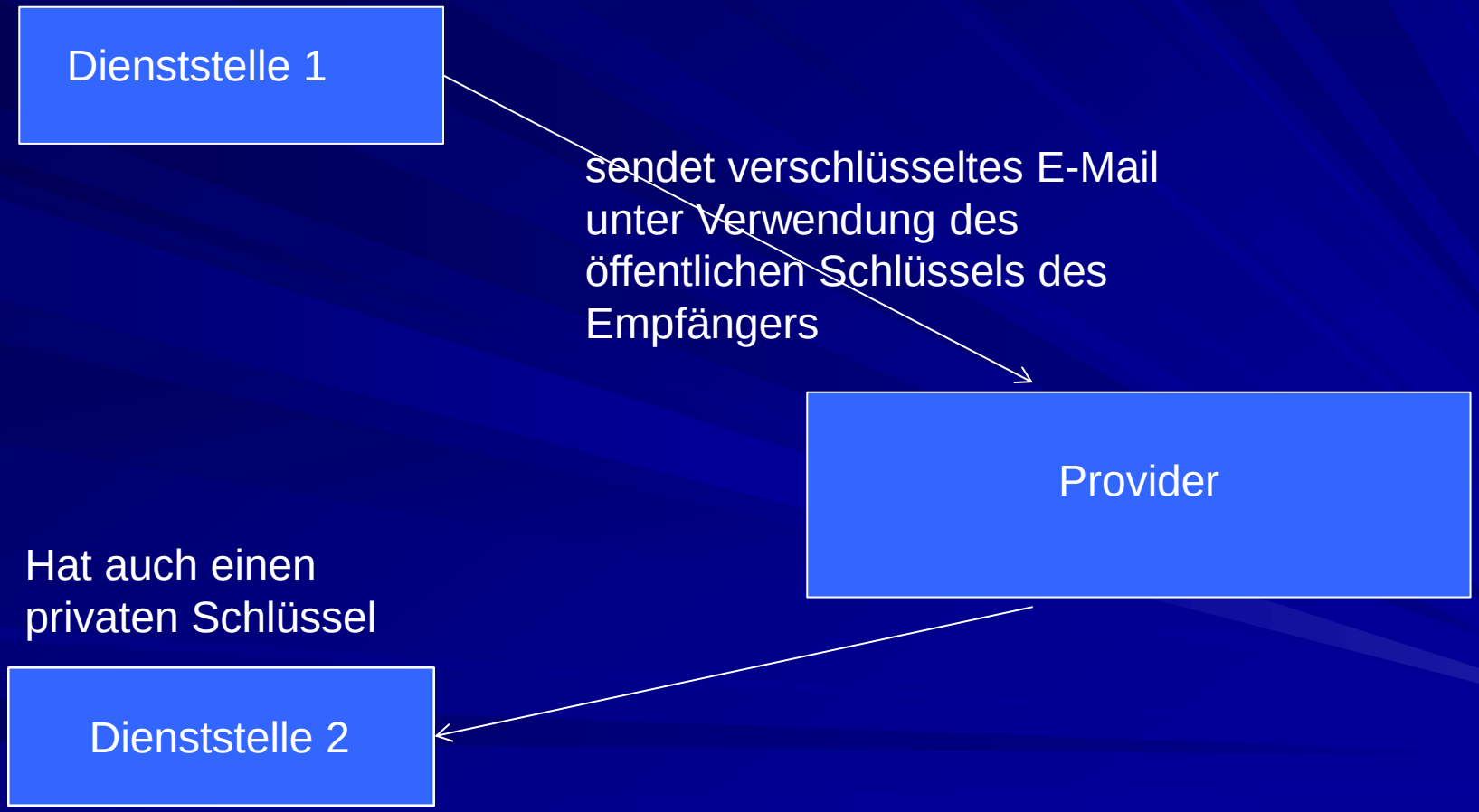
Gegenmaßnahmen und Sicherungen:

- Das „Idgard“-Prinzip: Der E-Mail-Verkehr zwischen kirchlichen (staatlichen, unternehmerischen) Dienststellen mit (beliebig vielen privaten) Teilnehmern wird über ein virtuelles privates Netzwerk abgewickelt:



Gegenmaßnahmen und Sicherungen:

- Punkt-zu-Punkt-Verschlüsselung:



Beispiel der Gothaer Versicherung

(1) Sie lassen sich von einer öffentlich anerkannten Stelle zertifizieren und erhalten einen privaten sowie einen öffentlichen Schlüssel

(2) Anschließend schicken Sie eine E-Mail an die Gothaer. (z.B. an info@gothaer.de). Diese E-Mail signieren Sie. Dadurch erhalten wir Ihren öffentlichen Schlüssel.

(3) Nun verfügen wir über Ihren öffentlichen Schlüssel und können Ihnen in Zukunft E-Mails verschlüsselt zuschicken. Diese können nur Sie mit Ihrem privaten Schlüssel öffnen.

Zusammenfassung und Beschluss der deutschen Diözesandatenschutzbeauftragten

- E-Mails, die dienstliche personenbezogene Daten enthalten, dürfen künftig nur verschickt werden
  - wenn zwischen Absender und Empfänger nur kirchliche Rechner vorhanden sind oder
  - wenn ein virtuelles privates Netzwerk einen Zugriff Dritter sicher ausschließt oder
  - wenn die E-Mails sicher verschlüsselt sind.

- E-Mails, die dienstliche personenbezogene Daten im Sinne des § 2 Abs. 10 KDO (besondere personenbezogene Daten) enthalten, dürfen künftig gar nicht verschickt werden.

Elektronische Kommunikation
Teil 2: Messenger

- Ein „Messenger“ ist eine Computeranwendung, die eine unmittelbare Kontaktaufnahme mit anderen im Internet eingeloggten Nutzern über Schrift, Sprache, Bildversendung oder sonstigen Digitalverkehr ermöglicht.
- Ausgangspunkt war der Windows Live Messenger, der vom Internet-Explorer unterstützt wurde, aber inzwischen kaum noch installiert ist.
- Der bisher erfolgreichste Messenger ist What‘s App mit ca. 1 Mrd. Nutzer.

What‘s App

- ist Teil des sozialen Mediums „Facebook“ und tauscht mit Facebook auch ungefragt Nutzerdaten aus.
- Weitere Probleme:
  - Physikalische Datenspeicherung außerhalb des EWR
  - Undurchsichtige Datenschutzbestimmungen
  - Verkauf von Nutzerdaten mehrfach nachgewiesen
- aber: Telefonfunktion und Verschlüsselung
- Beschluss der Diözesandatenschutzbeauftragten-Konferenz am 3.5.2017:

  Die Nutzung dienstlicher Daten mit What‘s App ist bundesweit untersagt.

Alternative Messenger

- s. zunächst die Zusammenstellung unter https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern
- Threema gilt als sicherer Messenger und unterliegt dem relativ strikten Schweizer Recht; Datenspeicherung in der Schweiz und damit im Gebiet des EWR, Verschlüsselung, Preis 0,99€
- Free Message (kostenlos), wird von United Internet vertrieben (1und1, GMX, Web.de), Verschlüsselung, Datenspeicherung in Deutschland.