EU-Datenschutz-Grundverordnung (DS-GVO)

Wichtige Handlungsfelder für Unternehmen

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

BvD e.V.
DATENSCHUTZ GESTALTEN

Inhalt

- Einleitende Hinweise
- Das Umstellungsprojekt in Phasen
- Aufgaben des Datenschutzbeauftragten nach DS-GVO
- Kurzprofil des BvD

Inhalt

- Einleitende Hinweise
- Das Umstellungsprojekt in Phasen
- Aufgaben des Datenschutzbeauftragten nach DS-GVO
- Kurzprofil des BvD

EU-Datenschutzrecht: EU-DS-GVO

Die EU-Datenschutz-Grundverordnung (DS-GVO, bzw. engl. GDPR – General Data Protection Regulation) bildet die Basis eines gemeinschaftlichen Verständnisses des Datenschutzes in den EU-Mitgliedsstaaten.

- Die gesetzlichen Vorgaben der DS-GVO müssen in allen Mitgliedsstaaten erfüllt werden.
- Öffnungsklauseln in der DS-GVO erlauben den Mitgliedsstaaten bis 25.05.2018 spezifischere Regelungen zu erlassen.
- Jeder Mitgliedsstaat startet von einer anderen Ausgangsposition basierend auf dem geltenden nationalstaatlichen Datenschutzrecht.

Nationales Datenschutzrecht: DSAnpUG-EU

Das BDSG n.F. regelt spezielle Bereiche des nationalen Datenschutzrechts auf der Basis der DS-GVO.

- In Deutschland wurde im Rahmen des Datenschutz-Anpassungs- und –Umsetzungsgesetz EU auch das neue Bundesdatenschutzgesetz am 12.05.2017 beschlossen und am 05.07.2017 im Bundesgesetzblatt veröffentlich.
- Art. 26 BDSG n.F.: Spezifizierung des Beschäftigtendatenschutzes auf Basis der Öffnungsklausel in Art. 88 D-SGVO
- EU-DSGVO und BDSG n.F. bilden zusammen die Grundlage für den Beschäftigtendatenschutz (inkl. datenschutzrechtlicher Anforderungen an Kollektivvereinbarungen)

… andere Mitgliedsstaaten werden dem Beispiel folgen.

Praxis des Datenschutzes in drei Akten!

Praxis des Datenschutzes in drei Akten!

Praxis des Datenschutzes in drei Akten!

Jeder im Unternehmen ist für den Datenschutz mitverantwortlich. Die Geschäftsführung trifft die Gesamtverantwortung – sie muss die Rechtmäßigkeit der Datenverarbeitung jederzeit nachweisen können und dazu die geeigneten Maßnahmen ergreifen!

Ausgangssituation der Unternehmen in Deutschland

Umsetzung des bisherigen BDSG

- Nach Schätzungen des BvD haben etwa **30% der Unternehmen** in Deutschland **das BDSG bislang nicht umgesetzt** und kennen dessen Regelungen nicht.
- Weitere **30%** haben nach Erfahrungen der BvD-Mitglieder **nur Teile des BDSG umgesetzt oder / und einen Alibi-Datenschutzbeauftragten bestellt**.
- Etwa **40% der Unternehmen** sind nach dem alten BDSG **datenschutzrechtlich gut aufgestellt**.

Ausgangssituation der Unternehmen in Deutschland

Umsetzung des bisherigen BDSG

Mit anderen Worten: 40 % der Unternehmen in Deutschland können den Umstieg auf die DS-GVO aus einer guten Startposition beginnen – und sind bereits mitten im Umstellungsprojekt. In den anderen Unternehmen müssen im Umstellungsprojekt auch die Versäumnisse der Vergangenheit aufgeholt werden. Dementsprechend höher sind Kosten und Kapazitätsbedarf in diesen Unternehmen.

Inhalt

- Einleitende Hinweise
- Das Umstellungsprojekt in Phasen
- Aufgaben des Datenschutzbeauftragten nach DS-GVO
- Kurzprofil des BvD

Das Umstellungsprojekt zur DS-GVO – Hinweise

Die Anpassung der Organisation an die Anforderungen des neuen europäischen und nationalen Datenschutzrechts sollte im Rahmen eines Organisationsprojektes erfolgen:

- Die Unternehmensleitung trägt die Verantwortung für die Umsetzung der rechtlichen Anforderungen. Sie sollte daher einen geeigneten Projektleiter für das Umstellungsprojekt benennen oder selbst die Leitung übernehmen. **Aufgrund der relativ knappen Zeit werden kurze Entscheidungswege benötigt**.
- Sämtliche Fachbereiche, die personenbezogene Daten verarbeiten, müssen in das Projekt eingebunden werden.

Das Umstellungsprojekt zur DS-GVO – Hinweise

Die Anpassung der Organisation an die Anforderungen des neuen europäischen und nationalen Datenschutzrechts sollte im Rahmen eines Organisationsprojektes erfolgen:

- Für größere Unternehmen bzw. solche mit komplexen Strukturen (Standorte, Verschachtelungen, …) empfiehlt es sich, eine Datenschutzorganisation mit festen Ansprechpartnern einzurichten (bspw. Datenschutzkoordinatoren), diese können die Ansprechpartner für die datenverarbeitenden Fachbereiche sein.
- Der betriebliche Datenschutzbeauftragte berät das Projekt fachlich und prüft die Umsetzung der gesetzlichen Anforderungen.
- Soweit ein Betriebsrat vorhanden ist, sollte dieser in das Projekt eingebunden werden.

Das Umstellungsprojekt zur DS-GVO

Die Projektphasen

Phase 1

Vorbereitung, Planung und Beauftragung des Projekts

Phase 2

Definition und Bearbeitung der Arbeitspakete und Einzelaufgaben (Projektbearbeitung)

Phase 3

Übergabe des Projekts in das Datenschutz-Tagesgeschäft

Maßnahmenplan zur Umsetzung – Phase 1

Vorbereitungsphase

1.1 Vorstellung für Geschäftsführung / Management Board

- ☐ 1.1.1 Vorstellung Projekt, Darstellung der Projektziele
- ☐ 1.1.2 Darstellung der benötigten Funktionen
- ☐ 1.1.3 Grobplanung von Maßnahmen und Ressourcen

1.2 Definition und Erteilung des **Projektauftrags für Umsetzungsphase**

- ☐ 1.2.1 Arbeitspakete und -gruppen festlegen
- ☐ 1.2.2 Bereitstellung benötigter Ressourcen (personell, finanziell)

1.3 Definition und Erteilung des **Projektauftrags für Implementierung eines Datenschutz-Managementsystems**

- ☐ 1.3.1 Arbeitspakete und -gruppen festlegen
- ☐ 1.3.2 Bereitstellung benötigter Ressourcen (personell, finanziell)

Maßnahmenplan zur Umsetzung – Phase 1

Vorbereitungsphase

1.4 Inventur / GAP-Analyse

- ☐ 1.4.1 Identifikation der Verfahren der Datenverarbeitung (Prozesse, Applikationen, Verarbeitungen)
- ☐ 1.4.2 Identifikation / Zuordnung Verfahrenseigner (processing activity owner) und Ansprechpartner
- ☐ 1.4.3 Bestandsaufnahme bestehender Verfahren (inkl. zugeh. Prozessen, Zwecken, Rechtsgrundlagen und Löschfristen)
- ☐ 1.4.4 Identifikation aller Auftragsverarbeiter / Subauftragsverarbeiter (inkl. zugehöriger ADV-Verträge sowie aller damit verbundenen Datentransfers mit Drittlandsbezügen
- ☐ 1.4.5 Identifikation aller sonstigen Drittlandsbezüge und internationalen Datentransfers
- ☐ 1.4.6 Ermittlung ggf. vorhandener Datenschutzprozesse / Dokumentationen

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.1 Erstellung des Verzeichnisses der Verarbeitungstätigkeiten (records of processing activities) und Ermittlung des Anpassungsbedarfs

- ☐ 2.1.1 Prüfung auf Einhaltung der Datenschutz-Grundsätze
- ☐ 2.1.2 Prüfung auf Umsetzung der Datensicherheitsmaßnahmen
- ☐ 2.1.3 Prüfung auf Umsetzung von Privacy-by-Design / Privacy-by-Default
- ☐ 2.1.4 Entwicklung eines Prozesses für die Risikoanalyse jeder Verarbeitungstätigkeit
- ☐ 2.1.5 Entwicklung eines Prozesses für die Datenschutzfolgenabschätzung
- ☐ 2.1.6 Entwicklung der Prozesse für die Umsetzung der Informationspflichten zu jeder Verarbeitungstätigkeit
  - ☐ a) bei Erhebung direkt beim Betroffenen
  - ☐ b) bei Erhebung bei Dritten

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.2 Entwicklung der Prozesse zur Wahrung der Betroffenenrechte

Festlegung und Dokumentation der Prozesse, inkl. Vorgehen zur Identitätsfeststellung des Berechtigten und Wahl des Kommunikationsmittels je Betroffenengruppe

- ☐ 2.2.1 Recht auf Auskunft (siehe Beispiel)
- ☐ 2.2.2 Recht auf Berichtigung
- ☐ 2.2.3 Recht auf Löschung / Recht auf Vergessen werden
- ☐ 2.2.4 Recht auf Einschränkung der Verarbeitung

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.2 Entwicklung der Prozesse zur Wahrung der Betroffenenrechte

Festlegung und Dokumentation der Prozesse, inkl. Vorgehen zur Identitätsfeststellung des Berechtigten und Wahl des Kommunikationsmittels je Betroffenengruppe

- ☐ 2.2.5 Benachrichtigungspflicht (abgeleitetes Recht bzgl. 2.2.2, 2.2.3, 2.2.4)
- ☐ 2.2.6 Recht auf Datenübertragbarkeit
- ☐ 2.2.7 Recht auf Widerspruch
- ☐ 2.2.8 Abgeleitete Pflichten bzgl. Ausnahme vom Verbot der automatisierten Einzelentscheidung

Beispiel: Recht auf Auskunft (Art. 15 DS-GVO)

Festlegung und Dokumentation der Prozesse, insbesondere der Verantwortlichkeit sowie Sicherstellung der Einhaltung der Pflichten beim Auftragsverarbeiter, sofern vorhanden (Beispiele: Payroll, Bewerbermanagement, Ticketsystem, etc.)

- Kommunikation mit der betroffenen Person in klarer und einfacher Sprache
- **bei Tätigwerden**:

  Unverzüglich, in jedem Fall innerhalb eines Monats (Fristverlängerung um zwei Monate nur falls aufgrund Komplexität und Anzahl der Anträge erforderlich und mit begründeter Information an die betroffene Person innerhalb eines Monats)
- **bei Nicht-Tätigwerden**:

  Begründete Unterrichtung der betroffenen Person ohne Verzögerung, spätestens innerhalb eines Monats.
- Bestätigung über Verarbeitung oder keine Verarbeitung (wenn keine Daten vorliegen) an den Betroffenen erteilen

Beispiel: Recht auf Auskunft (Art. 15 DS-GVO)

- **Inhalt der Auskunftserteilung, falls Bestätigung positiv:**
  - Verarbeitungszwecke
  - Kategorien pb Daten
  - Empfänger oder Kategorien von Empfängern insb. in Drittländern
  - Geplante Speicherdauer (falls möglich, andernfalls Kriterien für die Festlegung der Speicherdauer)
  - Bestehende Betroffenenrechte (Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch)
  - Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
  - alle verfügbaren Informationen über die Herkunft der Daten, falls Erhebung nicht bei der betroffenen Person
  - aussagekräftige Informationen über die involvierte Logik sowie die Trageweite und die angestrebten Auswirkungen der Verarbeitung für die betroffene Person, falls Verarbeitung mittels automatisierter Entscheidungsfindung
  - die geeigneten Garantien im Rahmen einer Übermittlung in Drittländer, falls Drittlandübermittlung erfolgt

Beispiel: Recht auf Auskunft (Art. 15 DS-GVO)

- Form der Auskunftserteilung
  - Auskunftserteilung durch Erstellung einer Kopie (weitere Kopien entgeltpflichtig)
  - Bei elektronischer Anfrage Auskunftserteilung in einem gängigen elektronischen Format, falls betroffene Person nichts anderes angibt
  - Nur mittels datenschutzkonformer Informationsmittel und innerhalb der Frist
- Sicherstellung der Auskunft ausschließlich an Berechtigte (Identität prüfen)
- Sicherstellung der Auskunftserteilung ohne Beeinträchtigung der Rechte und Freiheiten anderer Personen
- Unter Berücksichtigung der Ausnahmen gem. §§ 27, 28, 29 und 34 BDSG-neu

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.3 Entwicklung eines Data-Breach-Prozesses und der daraus abgeleiteten Informationspflichten unter Berücksichtigung möglicher Ausnahmen (Meldepflichten bei Datenpannen)

- ☐ 2.3.1 Meldungsweg innerhalb der Organisation (DSB, CISO, GF, etc.) bspw. innerhalb von 48 Stunden
- ☐ 2.3.2 Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden
- ☐ 2.3.3 Benachrichtigung der betroffenen Person

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.4 Prozess für das Einwilligungsmanagement (Beschäftigte / Dritte)

- ☐ 2.4.1 Festlegung und Dokumentation der Prozesse, inkl. Vorgehen zur Identitätsfeststellung des Einwilligenden und Wahl der Form der Einwilligungserklärung je Betroffenengruppe
- ☐ 2.4.2 Prüfung auf Einhaltung der Vorgaben an Freiwilligkeit und konkrete Informierung
- ☐ 2.4.3 Prüfung auf Eindeutigkeit und Nachweisbarkeit der Erteilung der Einwilligung
- ☐ 2.4.4 Prüfung auf Beachtung der Altersgrenzen bei Einwilligung Minderjähriger
- ☐ 2.4.5 Prüfung auf Wirksamkeit des Widerrufs einer Einwilligung mit Wirkung für die Zukunft

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.5 Auftragsverarbeiter-Rahmenbedingungen sicherstellen und Auftragsverarbeitungsmanagement um Datenschutzprozesse erweitern (auch bei inter-company-Verträgen)

- ☐ Prüfung, Aktualisierung und Nachverhandlung bestehender Verträge bezüglich der Mindestvorgaben der DS-GVO
- ☐ In der Rolle des Verantwortlichen (Auftraggebers): Sicherstellung der Einhaltung der Pflichten durch den Auftragsverarbeiter (Auftragnehmer)
  - ☐ Sorgfältige Auswahl des Auftragsverarbeiter
  - ☐ Regelmäßige Überprüfung, ob die rechtlichen Verpflichtungen durch die Auftragsverarbeiter eingehalten werden
- ☐ In der Rolle des Auftragsverarbeiters: Sicherstellung der Einhaltung der Pflichten gegenüber dem Verantwortlichen

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.6 Bestehende Betriebsvereinbarungen auf Konformität mit der DS-GVO und dem BDSG n.F. prüfen und ggf. nachverhandeln und anpassen

2.7 Erstellung der Datenschutz-Policy sowie spezifischer Datenschutz -Richtlinien (RL) bzw. Anpassung vorh. Richtlinien

- ☐ 2.7.1 Unternehmenspolitik zum Datenschutz dokumentieren
- ☐ 2.7.2 RL Auftragsverarbeitung,
- ☐ 2.7.3 RL Führung Verzeichnis der Verarbeitungstätigkeiten,
- ☐ 2.7.4 RL Beachtung datenschutzrechtlicher Vorgaben im Prozessdesign,
- ☐ 2.7.5 RL Change Management,
- ☐ 2.7.n RL ...

Maßnahmenplan zur Umsetzung – Phase 2

Definition und Bearbeitung der Arbeitspakete der Umsetzungsphase

2.8 Mitarbeiterschulungskonzept entwickeln

- ☐ 2.8.1 Webtraining
- ☐ 2.8.2 Präsenzschulungen für z. B. HR, Einkauf, IT

2.9 Datenübermittlung (EU / international) gruppenintern wie -extern auf Konformität mit der DS-GVO prüfen und ggf. notwendige Anpassungen vornehmen

Maßnahmenplan zur Umsetzung – Phase 3

Übergang des Projekts in laufende Tätigkeiten im Bereich Datenschutz

- ☐ 3.1 Rechtsfortschreibung monitoren und entsprechend berücksichtigen (Gesetzgebung und Rechtsprechung)
- ☐ 3.2 Ständige Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten und der Policies / Richtlinien
- ☐ 3.3 Regelmäßige Durchführung von Audits und Mitarbeitertrainings
- ☐ 3.4 Pflege des Kontakts mit Behörden und betroffenen Personen, insb. bei zwingender Konsultation
- ☐ 3.5 PDCA-Zyklus für das Datenschutz-Managementsystem (DSMS) sicherstellen und KVP-Prozess etablieren – dies ermöglicht die Darstellung der rechtmäßigen Datenverarbeitung, bspw. durch regelmäßige Audits und die dokumentierten Verbesserungen (analog Qualitätsmanagement)

Inhalt

- Einleitende Hinweise
- Das Umstellungsprojekt in Phasen
- Aufgaben des Datenschutzbeauftragten nach DS-GVO
- Kurzprofil des BvD

Aufgaben des Datenschutzbeauftragten (DSB) nach DS-GVO

- **Unterrichtung und Beratung** des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;
- **Überwachung der Einhaltung der gesetzlichen Vorgaben** aus der DS-GVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten **sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten** einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

Aufgaben des Datenschutzbeauftragten (DSB) nach DS-GVO

- **Beratung** — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung **und Überwachung** ihrer Durchführung gemäß der unionsrechtlichen und nationalrechtlichen Vorgaben.
- **Zusammenarbeit mit der Aufsichtsbehörde. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde** für mit der Verarbeitung zusammenhängende Fragen, einschließlich der Konsultation im Rahmen der Datenschutzfolgen-abschätzung.
- Gegebenenfalls **Beratung** zu allen sonstigen datenschutzrechtlichen Fragen.
- Der Datenschutzbeauftragte berät im Umstellungsprojekt und prüft die Ergebnisse hinsichtlich der datenschutzrechtlichen Anforderungen. Aus diesem Grund sollte er im Projekt keine leitende Funktion einnehmen (Interessenskonflikt).

Inhalt

- Einleitende Hinweise
- Das Umstellungsprojekt in Phasen
- Aufgaben des Datenschutzbeauftragten nach DS-GVO
- Kurzprofil des BvD

BvD – Eckdaten

- Gründung 1989 in Ulm
- Sitz seit 2006 in Berlin
- rund 950 Mitglieder
- 9 Arbeitskreise
- 10 Regionalgruppen
- 2 Ausschüsse

„Datenschutz wird in der digitalen Gesellschaft immer wichtiger. Der BvD begleitet die Umsetzung der neuen DS-GVO in deutsches Recht aktiv und engagiert sich für die Datenschutzbeauftragten.“

Thomas Spaeing,
BvD-Vorstandsvorsitzender

Auswahl der Aufgaben des BvD

- Aktiver Einsatz für die Etablierung des Berufsbildes „Datenschutzbeauftragter“ in Deutschland
- Regelmäßige Informationen an Entscheider aus Wirtschaft und Politik über das Berufsbild sowie die Leistungen des Datenschutzbeauftragten
- Permanenter Austausch mit Vertretern aus Verbänden, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Politik
- Gezielte Öffentlichkeitsarbeit bei wichtigen Gesetzgebungsverfahren
- Förderung der beruflichen Interessen unserer Mitglieder
- Umfangreiche Programme zur Fortbildung für Mitglieder
- Kompetente Unterstützung bei der täglichen Berufsausübung

DS-GVO

- Umfangreiches Informationsmaterial und Links auf der BvD-Website
- Management-Informationen für Mitglieder
- Stellungnahmen, Pressemitteilungen
- Positionspapiere
- Informationsveranstaltungen bundesweit
- Informationsveranstaltung in Brüssel mit EU-Abgeordneten und Datenschutzexperten

Initiative des BvD „Datenschutz geht zur Schule“ (DSgzS)

Kennzahlen

- 10.000 Schülerinnen und Schüler p.a.
- über 50 Dozentinnen und Dozenten bundesweit

Entwicklung Lehrerhandout

- in Kooperation mit klicksafe

Aktionstage

- Safer Internet Day (SID)
- Aktionstag vor Dozententag

Dozententag

- Jahrestreffen & Austausch

Die Initiative „Datenschutz geht zur Schule“ wird seit Oktober 2015 von der DATEV-Stiftung Zukunft gefördert.

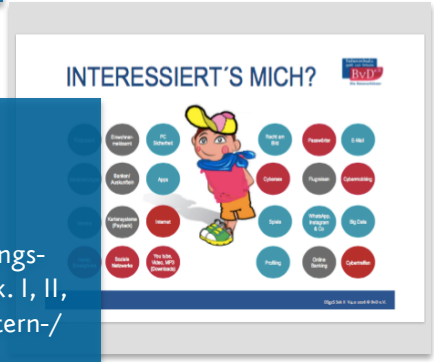
Materialien
„Datenschutz geht zur Schule“ (DSgzS)

Webcamsticker

- Abdeckung/Schutz der Kamera an PC, Tablet oder Smartphone

Lehrerhandout

- Unterrichtsmaterial für Lehrer (begleitend zum Foliensatz)



Foliensätze

- Für Sensibilisierungs-veranstaltungen (Sek. I, II, Berufsschule und Eltern-/ Lehrervortrag)

Flyer

- Informationen für Schulen und Sponsoren

Datenschutz Medienpreis (DAME)
Einsendeschluss 1. November 2017

Der BvD lobt einen Filmpreis für Datenschutz aus.

Damit alle in der komplexen digitalen Welt gleiche Chancen auf den Schutz persönlicher Daten haben, muss Datenschutz verständlich erklärt werden. Die Gesetze müssen bei den Bürgern ankommen, Regelungen verständlich und transparent sein. Ziel des Preises ist es, das öffentliche Interesse für das Thema Datenschutz rund um zu fördern. Ausgezeichnet werden Beiträge, die Datenschutz verständlich darstellen und zugleich anschaulich erklären.

DATENSCHUTZ MEDIENPREIS (DAME)

des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

2017 DAME BvD DATENSCHUTZ MEDIENPREIS

Jetzt einreichen!
Einsendeschluss
1. November 2017

Kontakt

Geschäftsstelle Berlin

Berufsverband der
Datenschutzbeauftragten (BvD) e.V.
Budapester Straße 31
10787 Berlin

Telefon (0 30) 26 36 77 60
Telefax (0 30) 26 36 77 63

E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de

Vorstand:

Thomas Spaeing, Vorsitzender
Jürgen Hartz, stell. Vorsitzender
Rudi Kramer, stell. Vorsitzender

Beisitzer: Dr. Jens Eckhardt,
Dr. Kai-Uwe Loser, Nikolaus Schrenk

Zuständig für die Initiative „Datenschutz geht zur Schule“: Rudi Kramer