Kommende Termine

09. Juni 2018	NatFak-Festival
12. Juni 2018	Spieleabend
21. Juni 2018	MatheParty

FACHSCHAFT MATHEMATIK

Alle Protokolle im Internet: www.fsmath.uni-bonn.de

Protokoll der FSR-Sitzung vom 06. Juni 2018

Beginn:	18.15 Uhr
Ende:	21.00 Uhr
Anwesende:	Tim Racs (Top 4), Benjamin Nettesheim, Valentin v. Bornhaupt, Antonia Ellerbrock, Carolin Büchting, David Göckede (Bis Top 3), Paul Stahr (Bis Top 3), Fabien Nießen (Ab Top 3), Robin Louis (Bis Top 3), Janna Schmidt, Lin Bachmann (Nach Top 1), Maria Matveev, Antonia Körner, Alex Dyck , Helene Glöckner (Bis Top 3), Marena Richter, Lena Berster, Leona Schlöder (während Top 1 gekommen), Lisa Franz (während Top 1 und Top 2), Michael Fedders (zwischen Top 2-3)
Sitzungsleitung:	Helene Glöckner bis Top 3, danach Benjamin Nettesheim
Protokoll:	Valentin v. Bornhaupt

TOP 0: Hallo

Helene eröffnet die Sitzung. Sie ist die Vertretung von Miriam. Es wird das Protokoll vom 09.05.2018 abgeklopft.

TOP 1: Berichte

Fachschaftenkonferenzsitzung Lin berichtet von der FK-Sitzung. Themen waren u.A. DSGVO, neues Hochschulgesetz und die neue „BASIS“-Website. Näheres siehe Anhang und FID 832.

EPG Helene berichtet, dass die EPG stattgefunden hat. Miriam und sie wollen auf der nächsten Fachgruppensitzung einen Antrag stellen, papiergestützte Evaluationen durchzuführen.

KoMa Marena berichtet von der KoMa: Sie war in einem Depressions-AK: Eine Fachschaft hat eine feste Vertrauensperson innerhalb der Fachschaft, die (gerade Fachschaftlern) als Ansprechpartner zur Verfügung stehen soll.

Benjamin berichtet von einer Resolution die an Regierungen appeliert, dass Tutoren eine Arbeitsrechtsbelehrung bekommen sollen. Außerdem gab es eine Resolution zu den Arbeitszeiten von Tutoren: Sie sollen so viel abrechnen können, wie sie gearbeitet haben. Eine dritte Resolution geht über die Änderung des Hochschulgesetzes. Sie spricht sich vor allem gegen die

Anwesenheitspflicht und Studienverlaufs-Vereinbarung aus.
Benjamin berichtet von einem AK bzgl. Online-Evaluationen. Einige Fachschaften waren in der Vergangenheit zu Online-Evaluationen gewechselt. Jedoch sind die meisten von ihnen auf Kurz oder Lang zu papiergestützten Evaluationen zurückgekehrt.
Außerdem war er in einem AK bzgl. Fachschafts-Master-Arbeit. Lena war in einem AK bzgl. Einbinden von Studenten in die Hochschulpolitik. Außerdem wurde sie darauf hingewiesen, dass eine FS hohe GEMA-Gebühren nachzahlen musste. Maria berichtet von einem CHE-AK. Antonia E. berichtet über einen Autismus-AK.
Benjamin war in einem AK Altklausuren. Er merkt an, dass ihm unser System gut gefalle. Außerdem war er in einem AK bzgl. KoMa-Orga: Hier kam die Überlegung auf, die Anzahl der Schlafplätze von KoMa-Besuchern einer Hochschule zu deckeln, damit von jeder Uni gleich viele Besucher kommen können. Näheres wird im Top KoMa besprochen.

Erstizeit Caro berichtet von einem Treffen mit Fabien, Vertretern der Physik-FS und Vertretern der Informatik-FS. Die Physiker, Informatiker und Mathematiker könnten ein gemeinsames 'Tri-Nerdisches-Turiner' veranstalten. Außerdem sei eine gemeinsame Party auf einem Boot denkbar.

Semester Rebreak Breakfast David berichtet vom SRB. Es war sehr schön, allerdings waren die Brötchen sehr schnell weg. Paul merkt an, dass man die Essensmenge nicht erhöhen sollte, weil der SRB nicht zum 'Sattessen' da sei. Helene merkt an, dass man Studenten sagen könnten, dass sie ihr eigenes Besteck mitnehmen sollten.

Lehramt KoMa Janna berichtet zu dem Thema Nachhaltigkeit im Lehramt. Leona merkt an, dass es neue Helpdesk-Angebote für Lehrämtler gäbe. Lisa ist eingeladen, um über die Grundzüge-Vorlesung zu berichten. Sie sagt, dass der Teil von Frau Kiesel gut verständlich war - der von Herrn Kaenders sei anspruchsvoll. Sie fühle sich ins kalte Wasser geworfen. Der Helpdesk wäre zu einer Zeit, in der kein Übungszettel verfügbar sei. Leona berichtet, dass das Modulhandbuch sehr schwammig gehalten sei. Außerdem sei die Fachliteratur im Modulhandbuch vermerkt. Lisa berichtet, dass die Klausur fair war. Sie habe das Gefühl, dass er Kritik an den Übungszetteln angenommen habe. Janna berichtet, dass sie in einem AK zum Thema „Nachhaltigkeit im Lehramt“war. Motivation, das Wissen zu behalten, sei ein elementares Problem ('Wofür brauche ich das später?'), aber genauso das Klischee, dass Lehrämtler dümmer seien (das sei verwurzelt bei Profs, Bachelor- und Lehramtsstudenten). Man sollte Freundschaften zwischen Bachelor-Studenten und Lehrämtlern fördern. Im jetzigen Studienverlaufsplan wäre es schwierig, entsprechende Freundschaften aufrechtzuerhalten. Näheres auf der FS-Fahrt.

TOP 2: Veranstaltungen

Spieleabend: Caro fragt, ob jetzt, wo wir eine neue Musikanlage haben, nicht jeden Spieleabend zu einem Karaoke-Spieleabend machen sollten. Paul merkt an, dass es Leute gibt, die wegen der Spiele kommen und von der Karaoke gestört werden könnten. Helene schlägt vor, das auf einer weniger vollen Sitzung zu besprechen, da der dieser Spieleabend ohne Karaoke angekündigt ist und deshalb auch so stattfinden sollte.
Antonia E. fragt nach einem großen Doppelkopf-Turnier. Das gibt Zustimmung. Es werden

für den kommenden Spieleabend folgende Schichten vergeben:

Zeit	**Personen**
Einkauf und Aufbau	Michael, Benjamin
18 - 19	Janna, Leona
19 - 20	Robin, Benjamin
20 - 21	Maria, Alex
21 - 22	Alex, Marena
Abbau	Toni E., Toni K.
Kneipe	David, Alex

FS-Fahrt: Es gibt 18 Teilnehmer. Wir brauchen noch weitere Autos, denn wir haben aktuell nur zwei bis drei Autos (Marena, (Janna), Paul). Evtl. müssten einzelne mit dem Zug fahren. Valentin organisiert das Kochen. Themen, die während der Fahrt besprochen werden sollen, sollen an Miriam gesendet werden. Es werden folgende Themen vorgeschlagen: Tutorenschulung, Modulberatung, Einladung zur Hochschulpolitik, FS-Zeitung, neue Veranstaltungsformate, Lehramt.

TOP 3: Fachschaftsübergreifende Erstiveranstaltungen

Helene ist gegen eine VA mit Alkohol-Pflicht. Antonia E. stellt klar, dass eine solche VA so nicht geplant sei. Die VA sei als Zusatz von unseren Ersti-VAs geplant. Termin wäre der 05.10.18, 15 oder 16 Uhr. Leona merkt an, dass die Zeit mit dem Programmiervorkurs kollidieren könnte. Das wird überprüft werden. Michael merkt an, dass man bei einer neuen Veranstaltung die Chance hätte, diese schon ohne Alkohol zu konzipieren. Das wäre weniger ausgrenzend, als alkoholische Spiele anzupassen (z.B. Flunkyball).
Ein Treffen mit anderen Fachschaften sei auch für 3. Semester interessant, weil diese so Kontakt zu anderen Fachschaften bekommen könnten.
Helene gibt die Sitzungsleitung an Benjamin ab.

Es wird ein Meinungsbild gebildet, wie wir dazu stehen, die Erstireferenten zu beauftragen, eine zusätzliche Veranstaltung mit den anderen FS zusammen zu planen. Es gibt einstimmige Zustimmung.

TOP 4: KOMA

OrgaMeta Maria berichtet, dass wir uns bereit erklärt haben, die KoMa 86, SS2020 auszurichten. Lena bemerkt, dass man 1,5 Jahre vor der KoMa anfangen sollte zu organisieren. Hierfür sei die Organisation von Schlafplätzen elementar. Wir dürften uns das Datum für diese KoMa aussuchen. Ob wir die KoMa tatsächlich 2020 ausrichten, erfahren wir bei der nächsten KoMa. Leona merkt an, dass man die Informatiker nach Erfahrungen von der KIF-Orga fragen kann/sollte. Maria merkt an, dass eine Gruppe bei Mattermost sinnvoll wäre. Caro bildet einen entsprechenden Arbeitskreis.

Vertrauensperson Marena berichtet von dem Vertrauenspersonen-AK. Es geht um eine Person, die bei Dingen, die man sich nicht traut, innerhalb der FS anzusprechen, helfen kann. Leona merkt an, dass es viele Beratungsstellen an der Uni-Bonn gibt. Valentin merkt an, dass es sinnvoll

wäre, eine Liste von Beratungsstellen anzulegen. Lena schlägt vor, dass man das auf der FS-Fahrt klären könnte. Benjamin kommt zu dem Schluss, dass sich jeder Gedanken machen soll und man nächste Woche Personen bestimmen könnte.

FS-Zeitung Maria berichtet von einem AK, in dem es um einseitige Zeitungen im DIN A4-Format ging. Vorstellbar wäre ein Blatt mit interessanten Daten, lustigen Dingen und Rätseln, das man auf der Toilette aufhängen könnte . Toni E. möchte, dass man sich bis nächster Woche dazu Gedanken macht, ob man zu einem solchen AK gehören möchte.

TOP 5: Sonstiges

Besteck Bei VAs gibt es zu wenig Besteck. Es wird angemerkt, dass in der Küche oben viel Besteck liegt.

NatFak-Festival Am Samstag findet das NatFak-Festival statt.

FK-Vertretung FK Vertretung von Lin übernimmt am 11.06. Fabien, 18.06. Leona.

TOP 6: Anhänge

Im Anhang sind folgende Dokumente zu finden:

1. Eine Stellenbeschreibung des Fachschaftenreferats, dass dringend neue Mitglieder sucht.
2. Ein Schreiben bezüglich der Jurymitgliedsuche für den Initiativpreis 'Impulse für die digitalgestützte Lehre' (studentisches Mitglied + Stellvertreter)
3. ein Muster eines Verarbeitungsverzeichnisses, dass dazu dient, dass ein (möglicher) Fachschaften- und AStA-Datenschutzbeauftragter die benötigten Daten hat.

Das Fachschaftenreferat sucht Nachwuchs!

Im Folgenden werden wir aufschlüsseln welche Aufgabenbereiche frei werden und was du mitbringen solltest, wenn du dir die Arbeit vorstellen kannst:

Vorsitz:

Die wichtigste Position, die es zu besetzen gilt. Der Vorsitz ist das Gesicht des Fachschaftenreferates. Sowohl nach Innen, als auch nach Außen. Du bereitest die wöchentlichen Fachschaftenkonferenzen vor und leitest sie. Außerdem solltest du regelmäßig zu den zweiwöchentlichen Gesamt-Asta-Sitzungen erscheinen und bist das Verbindungsglied zum Studierendenparlament, dem Rektorat und anderen Gremien. Du bist derjenige, der die Arbeit der anderen Mitglieder des Referates koordinieren muss. Du solltest dich mit dem Arbeitsfeld der anderen Mitarbeiter vertraut machen um einen Überblick behalten zu können. Wenn Beschwerden der Fachschaften kommen, bist du derjenige der mit den Mitarbeitern redet um zu klären wo der Fehler lag.

AFsG:

Momentan besteht unser AFsG-Team aus drei Mitarbeiterinnen. Die AFsG, oder die Allgemeinen Fachschaftengelder sind die Gelder, die jeder Fachschaft je Semester zustehen. In dieser Position ist es Hilfreich keine Angst vor Excel und Zahlen zu haben. Du wirst Anträge auf ihre Vollständigkeit prüfen, sehen wie viel Geld jeder Fachschaft Satzungsmäßig zusteht und sehen ob die Fachschaften ihre Haushaltspläne ordentlich gestaltet haben. Viel Zeit wirst du darauf verwenden Finanzern zu erklären, wie eine ordentliche Haushaltsführung auszusehen hat, damit diese ihr Geld bekommen. Sorgfalt und in manchen Fällen auch Konfrontationsbereitschaft sind hier sehr von Nutzen! Außerdem organisieren das Finanzteam (AFsG+BFsG) des Fachschaftenreferates auch einmal im Jahr einen Finanzworkshop in dessen Rahmen ihr dieses Wissen an die Finanzer der Fachschaften weitergeben sollt.

BFsG:

Die BFsG, oder die Besonderen Fachschaftengelder sind die, welche die Fachschaften beantragen können um, von den AFsG unabhängige, zweckgebundene finanzielle Unterstützung zu erhalten. In dieser Position ist es, ähnlich wie bei den AFsG, hilfreich mit Zahlen umgehen zu können.

Wahlen:

Jede Fachschaft wählt mindestens einmal im Jahr und wenn sie Geld von uns haben wollen, dann halten sie sich auch an die Wahlordnung. Als Referent für Wahlen bist du die erste Adresse für Fragen rund um die Wahlordnung, den Wahlprozess und die Wahldokumente. In dieser Position bist du auch dafür verantwortlich einmal im Jahr einen Wahlen-Workshop zu veranstalten, in dem du den Wahlprozess erläuterst und die Wahlordnung entschlüsselst. Wenn eine Fachschaftswahl durchgeführt wurde ist es deine Verantwortung die Wahldokumente, die die Fachschaft uns zur Dokumentation ihrer Wahl schickt auf ihre Korrektheit zu prüfen, da die Fachschaften bis zur bestätigten Wahl keine Gelder erhalten können.

Liebes Fachschaftenreferat,

auch in diesem Jahr wird der Preis "Impulse für die digitalgestützte Lehre" verliehen und auch in diesem Jahr wird eine achtköpfige Jury entscheiden, wer den Preis erhalten soll. Im letzten Jahr waren Sie bereits so nett, und haben uns bei der Suche von zwei studentischen VertreterInnen unterstützt. Frau van Krüchten kann auch dieses Jahr wieder Teil der Jury sein, eine/n zweite/n studentische/n Vertreter/in benötigen wir noch. Es wäre prima, wenn Sie auch in diesem Jahr aus den Fachschaften jemanden finden könnten, der Interesse hat, in der Jury mitzuwirken.
Kurz zum Ablauf: Ende Mai läuft die Frist zur Antragstellung aus, alle Jury-Mitglieder erhalten dann alle Anträge zur Begutachtung und nehmen eine erste Kategorisierung vor (unbedingt förderungswürdig, förderungswürdig, bedingt förderungswürdig). Am 06.07. von 10-12 Uhr findet die Jury-Sitzung statt und der Preisträger 2018 wird ermittelt.

Es wäre also notwendig, dass der/die Vertreter/in am 06.07. an der Jury-Sitzung teilnehmen kann.

Für eine Rückmeldung vielen Dank!

Mit besten Grüßen
Jennifer Sobotta

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name	Allgemeiner Studierendenausschuss der Rheinischen Friedrichs-Wilhelms-Universität Bonn
Straße	Nassestraße 11
Postleitzahl	53113
Ort	Bonn
Telefon	0228 - 737030
E-Mail-Adresse	info@asta.uni-bonn.de
Internet-Adresse	

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name	
Straße	
Postleitzahl	
Ort	
Telefon	
E-Mail-Adresse	

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name	Vorsitzende des AStA Uni Bonn
Straße	Nassestraße 11
Postleitzahl	53113
Ort	Bonn
Telefon	0228 - 73 7037
E-Mail-Adresse	

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede	Frau
Titel	vakant
Name, Vorname	Nassestraße 11
Straße	53113
Postleitzahl	Bonn
Ort	0228 - 73 7030

Verarbeitungstätigkeit: Benennung:	**lfd. Nr.:**
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit	
Name des eingesetzten Verfahrens	
Rechtsgrundlage für das Verfahren	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	1. ☐ Beschäftigte 2. ☐ Interessenten 3. ☐ Lieferanten 4. ☐ Kunden 5. ☐ Patienten 6. ☐ 7. ☐ 8. ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	1. ☐ 2. ☐ 3. ☐ 4. ☐ Besondere Kategorien personenbezogener Daten (Art. 9): 1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐

Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion:
	☐ extern Empfängerkategorie:
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine inter-nationale Organisation (Art. 30 Abs. 1 S. 2 lit. e) Nennung der konkreten Datenempfänger Sofern es sich um eine in Art. 49 Abs. 1	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant. ☐ Datenübermittlung findet wie folgt statt: ☐ Drittland oder internationale Organisation (Name): ☐ Dokumentation geeigneter Garantien:
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit.	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung*

Verantwortlicher	Datum	Unterschrift

Technische und organisatorische Maßnahmen **gem. Artikel 32 Absatz 1 DSGVO für Verantwortliche (Artikel 30 Absatz 1 lit. G) und Auftragsverarbeiter (Artikel 30 Absatz 2 lit. D)**
1. Pseudonymisierung:
2. Verschlüsselung:
3. Gewährleistung der Vertraulichkeit:
4. Gewährleistung der Integrität:
5. Gewährleistung der Verfügbarkeit:
6. Gewährleistung der Belastbarkeit der Systeme:
7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall:
8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen:

Ausfüllhilfe für das Verzeichnis von Verarbeitungstätigkeiten

1. Zwecke der Verarbeitung, Art. 30 Abs. 1 S. 2 lit. b DS-GVO

Je Beschreibung einer Verarbeitungstätigkeit ist der Verarbeitungszweck zu dokumentieren, z. B.:

- Personalaktenführung/Stammdaten
- Lohn-, Gehalts- und Bezügeabrechnung
- Arbeitszeiterfassung
- Urlaubsdatei
- Nutzungsprotokollierungen IT/Internet/E-Mail
- Bewerbungsverfahren
- Telefondatenerfassung
- Firmenparkplatzverwaltung
- Videoüberwachung an Arbeitsplätzen, in Schulen etc.
- Schülerverwaltung, Unterrichtsplanung, Zeugniserstellung
- Beschaffung/Einkauf sowie Finanzbuchhaltung
- Antragsbearbeitung (Bauanträge, Wohngeldanträge etc.)
- Rats- und Bürgerinformationssysteme
- Meldewesen (Melderegister)
- Fahrerlaubnisregister und Fahrzeugregister
- Wahlen (Wählerverzeichnis)
- amtsärztliche Untersuchungen
- Schwangeren- und Mütterberatung
- Erfassung und Überwachung der nichtakademischen Heilberufe

Für jede Verarbeitung sind vorher die Zwecke festzulegen.
Die Zwecke müssen eindeutig und so aussagekräftig sein, dass die Aufsichtsbehörde die Angemessenheit der getroffenen Schutzmaßnahmen und die Zulässigkeit der Verarbeitung vorläufig einschätzen kann.

2. Kategorien betroffener Personen und personenbezogener Daten, Art. 30 Abs. 1 S. 2 lit. c DS-GVO

Zu beschreiben sind die Kategorien betroffener Personen und die Kategorien personenbezogener Daten. Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO sollte gesondert beschrieben werden (Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person).
Dabei empfiehlt es sich hinsichtlich der einzelnen Kategorien personenbezogener Daten laufende Nummern zu vergeben, die so eine Zuordnung zu den weiteren konkreten Angaben gem. Art. 30 Abs. 1 S. 2 lit. d bis g DS-GVO ermöglichen, z. B. zu konkreten Löschregeln.

Aufgegliedert z. B. in der Darstellung der „Kategorie Beschäftigte“ in die Daten-Kategorien:

- Mitarbeiter-Stammdaten mit Adressdaten, Geburtsdatum, Bankverbindung, Steuermerkmale, Lohngruppe, Arbeitszeit, bisherige Tätigkeitsbereiche, Qualifikationen etc.
- Bewerbungen mit Kontaktdaten, Qualifikationsdaten, Tätigkeiten etc.
- Arbeitszeugnisse mit Adressdaten, Leistungsdaten, Beurteilungsdaten etc.
- Abmahnungen mit Adressdaten, Arbeitsverhalten, Leistungsdaten etc.
- Betriebsarztuntersuchungen mit Adressdaten, Gesundheitsdaten etc.
- Stundenplan als Einsatzplan für Lehrkräfte
- Videoüberwachung an Arbeitsplätzen etc.

Aufgegliedert z. B. in der Darstellung der „Kategorie Kundendaten“ in die Kategorien:

- Kunden-Kontaktdaten mit Adressdaten, Ansprechpartnern etc.
- Kundengruppe/-interesse
- Umsatzdaten bisher
- Bonitätsdaten
- Zahlungsdaten usw.
- für Schulen: Fehlzeiten, Schulleistungsnachweise

Aufgegliedert z. B. in der Darstellung „Kategorie Abgeordnetendaten“ in die Kategorien:

- Namen und Kontaktdaten (Adresse, Telefon, E-Mail) von Abgeordneten
- Fraktionszugehörigkeit

3. Kategorien von Empfängern, Art. 30 Abs. 1 S. 2 lit. d DS-GVO

Zu beschreiben sind die Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen. Sie können z. B. für die Lohn- und Gehaltsabrechnung wie folgt aufgegliedert werden:

- Banken
- Sozialversicherungsträger
- Finanzämter
- unternehmensinterne andere Datenempfänger (z. B. Betriebsarzt, Personalrat)
- ggf. Gläubiger bei Lohn-/Gehaltspfändungen
- ggf. Träger der Betriebsrente
- ggf. Auftragsverarbeiter
- ggf. Muttergesellschaft

Empfänger können auch Teile eines Unternehmens oder einer Behörde sein. Dies ist der Fall, sofern ein Zugriff auf die Daten möglich ist (z. B. Zugriff auf Unternehmens- oder Kundendaten bei bundesweit tätigen Banken oder abgebende und aufnehmende Schule bei gleichem Schulträger).
Der Begriff „Datenempfänger“ ist daher zu ergänzen durch „Zugriffsberechtigte“. Die Angaben zu den zugriffsberechtigten Personen sind nach der DS-GVO zwar nicht vorgesehen. Es wird jedoch empfohlen, Angaben zu diesen zu machen.
Die Zugriffsberechtigten sollten, wie bisher, ohne namentliche Angabe angegeben werden. Sie müssen jedoch z. B. über eine Rollen- oder Funktionsbeschreibung eindeutig bestimmbar sein.

Zu „Drittländern“ sollte in jedem Fall eine Aussage getroffen werden, also auch angegeben werden, wenn eine Übermittlung in Drittländer nicht stattfindet und auch nicht geplant ist.
Eine Übermittlung in Drittländer erfolgt auch, wenn sich dort der Server befindet oder der Mailversand hierüber abgewickelt wird. Ebenso kann eine Übermittlung in Drittländer vorliegen, wenn Supportdienstleistungen aus diesem erbracht werden.
„Offenlegung“ bedeutet, dass sowohl die Empfänger in der Vergangenheit, als auch jene in der Zukunft zu benennen sind.

4. Übermittlungen in Drittländer – Art. 30 Abs. 1 S. 2 lit. e DS-GVO

Angaben zu Übermittlungen von personenbezogenen Daten in ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 DS-GVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien Empfänger in Drittländern und internationale Organisationen sind keine Kategorien und daher konkret zu benennen.
Art. 49 Abs. 6 DS-GVO ist zu beachten, wonach der Verantwortliche die von ihm vorgenommene Beurteilung sowie die angemessenen Garantien im Sinne des Art. 49 Abs. 1 Unterabsatz 2 DS-GVO im Verzeichnis der Verarbeitungstätigkeiten aufnimmt.

5. Speicherdauer – Art. 30 Abs. 1 S. 2 lit. f DS-GVO

Angabe der vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien, z. B.

- die geltenden handels- und steuerrechtlichen Aufbewahrungspflichten für Personaldaten, Kundendaten etc.
- geltende Aufbewahrungs- und Löschfristen für Schülerdaten, Prüfungsunterlagen etc.
- gesetzlich vorgesehene Löschungsfristen (z. B. § 14 Bundesmeldegesetz)
- vom Verantwortlichen festgelegte Überprüfungs-/Löschungsfristen

Ein allgemeiner Verweis auf Aufbewahrungspflichten genügt nicht, vielmehr sind präzise Angaben erforderlich.

6. Referenzdokumente

Es wird empfohlen, weitere Bausteine einer umfassenden Dokumentation der Datenschutzstrategie, wie z. B.

- die Dokumentation interner Verhaltensregeln,
- die Dokumentation einer Risikoanalyse oder allgemeinen Datensicherheitsbeschreibung,
- ein umfassendes Datensicherheits- oder Wiederanlaufkonzept,
- ein Zertifikat oder
- Ergebnisse einer Datenschutz-Folgenabschätzung

am Ende der Dokumentation der Verarbeitungstätigkeit unter „Sonstiges“ als Referenz anzugeben.
Auf Nachfrage können diese Referenzdokumente zusätzlich zum Verzeichnis der Aufsichtsbehörde vorgelegt werden; es ist sinnvoll, zumindest die für das Verständnis und die Bewertung des Verarbeitungsverzeichnisses essentiellen zusätzlichen Dokumente bereits im ersten Schritt freiwillig mitzuliefern. Insofern stellen die zusätzlich aufgeführten Dokumentationen keine Anlagen zum Verzeichnis dar, sondern weitere, darüber hinausgehende Bausteine einer umfassenden Dokumentation der organisationsinternen Datenschutzstrategie, auf welche verwiesen werden und die neben dem Verzeichnis vorgehalten werden können.

Sie dienen zusammen mit dem Verzeichnis der Umsetzung der aus Art. 5 Abs. 2 DS-GVO resultierenden Rechenschaftspflicht. Wird innerhalb des Verzeichnisses auf andere Dokumente, wie z. B. ein anderes Verarbeitungsverzeichnis Bezug genommen, so ist dies an dieser Stelle als Referenzdokument aufzuführen.
Es wird empfohlen, eine solche Dokumentation an zentraler Stelle zu pflegen.

7. Technische und organisatorische Maßnahmen Art. 30 Abs. 1 S. 2 lit. g DS-GVO

Trotz der Formulierung „wenn möglich“ stellt die allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO hier den Regelfall dar.
Art. 5 Abs. 2 DS-GVO verpflichtet den Verantwortlichen insbesondere auch zur Dokumentation der technischen und organisatorischen Maßnahmen (Art. 5 Abs. 1 lit. f DS-GVO). Zudem muss der Verantwortliche die Wirksamkeit dieser Maßnahmen regelmäßig überprüfen (Art. 32 Abs. 1 lit. d DS-GVO). Beide Forderungen kann der Verantwortliche nur erfüllen, wenn die technischen und organisatorischen Maßnahmen vollständig beschrieben sind (etwa in einem Sicherheitskonzept).
Eine Verarbeitung darf erst erfolgen, wenn der Verantwortliche seiner Pflicht nach Art. 24 DS-GVO nachgekommen ist. Darunter fallen neben den Verpflichtungen nach Art. 12 und 25 DS-GVO auch diejenigen nach Art. 32 DS-GVO zur Bestimmung und Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Das betrifft primär Fragen der Sicherheit der Verarbeitung, schließt somit aber auch Maßnahmen zur Gewährleistung von Betroffenenrechten ein. In das Verzeichnis ist eine allgemeine, einfach nachvollziehbare Beschreibung der für diesen Zweck getroffenen Maßnahmen aufzunehmen. Die Beschreibung der jeweiligen Maßnahme ist konkret auf die Kategorie betroffener Personen bzw. personenbezogener Daten im Sinne des Art. 30 Abs. 1 S. 2 lit. c DS-GVO zu beziehen, soweit eine entsprechende Differenzierung in ihrer Anwendung erfolgt.
Ist bei der Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zu erwarten, hat die Bestimmung der Maßnahmen bereits im Rahmen einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO zu erfolgen.
Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DS-GVO.
Nach Art. 32 Abs. 1 DS-GVO sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und Schwere der mit ihr verbundenen Risiken geeignete technische und organisatorische Maßnahmen zu treffen, um insbesondere Folgendes sicherzustellen:

8. Maßnahmenbereiche, die sich aus Art. 32 Abs. 1 DS-GVO ergeben:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste
- Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
- Wiederherstellung der Verfügbarkeit personenbezogener Daten und des Zugangs zu ihnen nach einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen

Nachfolgend werden den einzelnen Bereichen typische, bewährte technische und organisatorische Maßnahmen zugeordnet. Die Auflistung ist nicht vollständig oder abschließend. In Abhängigkeit von den konkreten Verarbeitungstätigkeiten können weitere oder andere Maßnahmen geeignet und angemessen sein. Auch ist die Zuordnung einzelner Maßnahmen zu einem bestimmten Maßnahmenbereich nicht in jedem Fall eindeutig.

- Maßnahmen zur Pseudonymisierung personenbezogener Daten Hierzu zählen u. a.:
  - Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
  - Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
  - Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungs-verfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
  - Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisierungsvorgänge
  - zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung eingehenden geheimen Parameter
  - Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
  - Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

- Maßnahmen zur Verschlüsselung personenbezogener Daten (z. B. in stationären und mobilen Speicher-/Verarbeitungsmedien, beim elektronischen Transport)

Schlüssel können flüchtig (z. B. für die Dauer eines Kommunikationsvorgangs) oder statisch (mittel- oder langfristig) für den Schutz personenbezogener Daten eingesetzt werden.
Es sind Festlegungen zu treffen (z. B. im Rahmen eines Kryptokonzepts) u. a. zur Auswahl geeigneter kryptografischer Verfahren und Produkte, zur Organisation ihres Einsatzes, zu Maßnahmen bei der Entdeckung von Schwächen in Verschlüsselungsverfahren oder -produkten (Um- oder Überverschlüsselung) sowie zu Schlüssellängen. Voraussetzung für effektive Verschlüsselung ist ein adäquates Schlüsselmanagement, das u. a. folgende Aspekte betrifft:

- zufällige Erzeugung der Schlüssel
- Autorisierung von Personen zur Verwaltung und zur Nutzung von Schlüsseln bzw. ihre Zuweisung zu Geräten, in denen sie eingesetzt werden
- zuverlässige Schlüsselverteilung, Verknüpfung von Schlüsseln mit Identitäten von natürlichen Personen oder informationstechnischen Geräten, ggf. Einbringen in speziell gesicherte Speichermedien (z. B. Chipkarten)
- Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
- regelmäßiger oder situationsbezogener Schlüsselwechsel, ggf. eine Schlüsselarchivierung, stets sorgfältige Schlüssellöschung nach Ablauf des Lebenszyklusses
- Verwaltung des Lebenszyklus der Schlüssel von Erzeugung und Verteilung über Nutzung bis zu ihrer Archivierung und Löschung

- Maßnahmen zur Gewährleistung der Integrität und Vertraulichkeit der Systeme und Dienste

Die folgenden Maßnahmen sollen eine spezifikationsgerechte Verarbeitung sichern und nicht autorisierte bzw. unberechtigte Verarbeitung sowie unbeabsichtigte Änderung, Verlust oder Schädigung personenbezogener Daten ausschließen; beim Verantwortlichen selbst oder auf

dem Transportweg zu Auftragsverarbeitern oder Dritten. Hierzu zählen u. a.:

- Formulierung von verbindlichen Sicherheitsleitlinien
- Definition der Verantwortlichkeiten für das Informationssicherheitsmanagement
- Inventarisierung der zu verarbeitenden personenbezogenen Daten
- Inventarisierung der Informationstechnik
- Erarbeitung eines Sicherheitskonzepts, ggf. unter Durchführung einer Risikoanalyse
- Personalsicherheit: Überprüfung und Verpflichtung des Personals, Sensibilisierung und Training, Aufgabentrennung
- Spezifikation der Sicherheitsanforderungen an Informationssysteme und deren Konfiguration, Prüfung ihrer Einhaltung
- Schutz vor unberechtigtem physischem Zugang, einschließlich Schutz von Mobilgeräten
- Erarbeitung eines Rollen- und Rechtekonzepts
- Maßnahmen zur Autorisierung von Personen für den Zugriff auf personenbezogene Daten und die Steuerung der Verarbeitung
- Zugriffskontrolle und sicherer Umgang mit Speichermedien, einschließlich der Maßnahmen zur zuverlässigen Authentisierung von Personen gegenüber der Informationstechnik, zur Sicherung der Revisionsfähigkeit der Eingabe und der Änderung von personen-bezogenen Daten sowie ggf. der Nutzung und des Zugriffs auf diese und zur Revision dieser Prozesse
- Maßnahmen der Betriebssicherheit, insbesondere zur Spezifikation der Bedienabläufe, zur Änderungssteuerung, zum Schutz vor Malware, zum Umgang mit technischen Schwachstellen, zur kontrollierten Installation und Konfiguration neuer Software, sowie zur Ereignisüberwachung und -protokollierung, einschließlich der regelmäßigen und anlassbezogenen Auswertung dieser Protokolle
- Maßnahmen, die (berechtigte oder unberechtigte) Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (z. B. Signaturverfahren, Hashverfahren)
- Maßnahmen zur Kommunikationssicherheit: Netzwerksicherheitsmanagement, insbesondere zur Kontrolle und Einschränkung des Datenverkehrs (Firewalls, Application Layer Gateways), Einrichtung von Sicherheitszonen, Authentisierung von Geräten gegeneinander
- sichere Gestaltung von Informationsübertragungen, einschließlich des Abschlusses von Vereinbarungen mit regelmäßigen Übermittlern und Empfängern personenbezogener Daten und der Authentisierung der Kommunikationspartner
- Sicherung und Überprüfung der Authentizität der übermittelten Daten
- sichere Einbeziehung von externen Diensten
- Management von Informationssicherheitsvorfällen
- Aufrechterhaltung der Informationssicherheit bei ungeplanten Systemzuständen
- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen
- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

- Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  Die folgenden Maßnahmen sollen sicherstellen, dass personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden. Hierzu zählen u. a.: Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts

  - Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
  - Dokumentation von Syntax und Semantik der gespeicherten Daten
  - Redundanz von Hard- und Software sowie Infrastruktur
  - Umsetzung von Reparaturstrategien und Ausweichprozessen
  - Vertretungsregelungen für abwesende Mitarbeiter

- Maßnahmen, um nach einem physischen oder technischen Zwischenfall (Notfall) die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen rasch wiederherzustellen

Eine besondere Ausprägung der Gewährleistung von Verfügbarkeit ist hinsichtlich möglicher Notfälle (siehe dazu auch BSI Standard 100-4) erforderlich. Hierzu sind u. a. folgende Maß-nahmen erforderlich:

- Erstellung und Umsetzung eines Notfallkonzepts
- Erarbeitung eines Notfallhandbuches
- Integration des Notfallmanagements in Geschäftsprozesse
- Durchführung von Notfallübungen
- Erprobung von Wiederanlaufszenarien

- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen Hierzu zählen u. a.:

  - regelmäßige Revision des Sicherheitskonzepts
  - Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung
  - Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme,
  - Externe Prüfungen, Audits und Zertifizierungen.

Helene Glöckner bis Top 3, danach Benjamin Nettesheim	Valentin v. Bornhaupt
Sitzungsleiter	Protokollant