MAX PLANCK
GESELLSCHAFT

DATENSCHUTZLEITLINIE
der Max-Planck-Gesellschaft

September 2021

DATA PROTECTION GUIDELINE
of the Max-Planck-Gesellschaft

September 2021

INHALT

1. Ziele

Die Max-Planck-Gesellschaft betreibt Grundlagenforschung in den Natur-, Bio-, Geistes- und Sozialwissenschaften im Dienste der Allgemeinheit. Der gesetzeskonforme Umgang mit personenbezogenen Daten ist eine Basis für eine vertrauensvolle Beziehung zu Studienteilnehmenden, Beschäftigten, zu Kooperations- und Geschäftspartnerinnen und -partnern sowie allen an der Forschung der Max-Planck-Gesellschaft interessierten Personen.

Die Max-Planck-Gesellschaft berücksichtigt bei ihren strategischen und operativen Entscheidungen die geltenden Datenschutzbestimmungen. Dabei berücksichtigt sie die mit Verarbeitungsvorgängen verbundenen Risiken für betroffene Personen in angemessener Weise.

2. Geltungsbereich

Diese Leitlinie ist Bestandteil des Datenschutzmanagementsystems der Max-Planck-Gesellschaft und beschreibt die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten und den Einsatz datenverarbeitender Systeme.

Sie ist verbindlich für alle Institute und Einrichtungen des Max-Planck-Gesellschaft e.V.[1] sowie für Externe, die als Dienstleistende oder Nutzende von datenverarbeitenden Systemen mitwirken.

3. Gesetzliche Anforderungen

Die Verarbeitung personenbezogener Daten ist in der EU Datenschutz-Grundverordnung (DS-GVO), dem Bundesdatenschutzgesetz (BDSG) sowie weiteren nationalen Vorgaben verbindlich geregelt. Diese Vorschriften haben insoweit Vorrang, falls die Einhaltung dieser Leitlinie zu einem Verstoß gegen diese Vorschriften führen würde.

4. Begriffsbestimmungen

4.1 personenbezogene Daten

Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Zu den besonderen Kategorien personenbezogener Daten zählen nach Art. 9 Abs. 1 DS-GVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

[1] Der Max-Planck-Gesellschaft e.V. empfiehlt rechtlich selbstständigen Einrichtungen, die mit ihm verbunden bzw. assoziiert sind, eine entsprechende Anwendung und Umsetzung der Datenschutzleitlinie in ihrem Verantwortungsbereich sicherzustellen.

4.2 Verarbeitung

Verarbeitung umfasst nach Art. 4 Nr. 2 DS-GVO jeden analogen oder digitalen Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

5. Verantwortlichkeiten

Die satzungsrechtliche Organisationsstruktur der Max-Planck-Gesellschaft sieht für die Umsetzung der datenschutzrechtlichen Vorgaben verschiedene zentrale und lokale Funktionsträger in der Verantwortung. Die gesetzlichen und satzungsmäßigen Vertreter des Max-Planck-Gesellschaft e.V.[2] tragen die rechtliche Verantwortung im Außenverhältnis. Sie üben insoweit die Funktion der Verantwortlichen gemäß DS-GVO und BDSG aus. Die Verantwortungsverteilung im Innenverhältnis erfolgt entsprechend der Satzung der Max-Planck-Gesellschaft. Dem Verwaltungsrat obliegt die Aufsichtsverantwortung, den Leitungsverantwortlichen der Einrichtungen und Institute die Umsetzungsverantwortung. Alle Beschäftigten tragen im Rahmen ihrer jeweiligen Verantwortlichkeiten dazu bei, die externen und internen Vorgaben bei der Erfüllung ihrer Tätigkeiten sicherzustellen. Die Max-Planck-Gesellschaft ist gesetzlich zur Benennung einer oder eines Datenschutzbeauftragten verpflichtet.

6. Grundsätze für jede Verarbeitung personenbezogener Daten (Art. 5 DS-GVO)

6.1 Rechtmäßigkeit

Personenbezogene Daten werden auf rechtmäßige Weise nach Treu und Glauben verarbeitet. Die Datenverarbeitung erfolgt nur, wenn gesetzliche Vorschriften der DS-GVO, des BDSG oder vorrangige Rechtsvorschriften dies anordnen, ausdrücklich zulassen oder eine Einwilligung der betroffenen Personen vorliegt.

6.2 Zweckbindung

Personenbezogene Daten werden nur für legitime Zwecke verarbeitet, die vor der Datenhebung definiert wurden. Nachträgliche Änderungen der Verarbeitungszwecke bedürfen einer erneuten Prüfung einer vorhandenen Rechtsgrundlage.

6.3 Transparenz

Die betroffenen Personen werden gemäß den gesetzlichen Vorgaben über die jeweilige Datenverarbeitung informiert. Die Information erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache.

6.4 Datenminimierung

Jede Verarbeitung personenbezogener Daten ist so gestaltet, dass sie sowohl quantitativ als auch qualitativ auf das für die Erreichung der Zwecke erforderliche Maß beschränkt ist. Sofern der Zweck es zulässt und der Aufwand in einem angemessenen Verhältnis zum angestrebten Ziel steht, werden anonymisierte Daten verwendet.

[2] Dies sind der Vorstand gemäß § 26 BGB i.V.m. § 17 Abs. 1 der Satzung der Max-Planck-Gesellschaft sowie die Wissenschaftlichen Mitglieder mit Leitungsfunktion gemäß § 30 BGB, § 28 Abs. 3 der Satzung.

6.5 Richtigkeit

Personenbezogene Daten werden sachlich richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand verarbeitet. Mittels angemessener Maßnahmen wird sichergestellt, dass unrichtige, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

6.6 Speicherbegrenzung

Personenbezogene Daten werden grundsätzlich nur so lange verarbeitet, wie dies für die Erfüllung der jeweiligen Zwecke erforderlich ist und keine anderweitigen gesetzlichen, vertraglichen oder satzungsgemäßen Aufbewahrungspflichten bestehen.

6.7 Sicherheit der Datenverarbeitung

Personenbezogene Daten werden durch angemessene technische und organisatorische Maßnahmen vor unberechtigtem Zugriff oder Offenlegung, unrechtmäßiger Verarbeitung sowie versehentlichem Verlust, Veränderung oder Zerstörung geschützt. Diese Maßnahmen berücksichtigen den Stand der Technik, die Risiken der Verarbeitung und den Schutzbedarf. Die Anforderungen an die Maßnahmen sind Teil des Informationssicherheitsmanagements der Max-Planck-Gesellschaft.

7. Sicherstellung der Betroffenenrechte

Alle betroffenen Personen haben gegenüber der Max-Planck-Gesellschaft im Rahmen der gesetzlichen Vorgaben die folgenden Rechte:

- Recht auf Auskunft (Art. 15 DS-GVO)
- Recht auf Berichtigung (Art. 16 DS-GVO)
- Recht auf Löschen (Art. 17 DS-GVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)
- Recht auf Datenübertragbarkeit (Art. 19 DS-GVO)
- Recht auf Widerspruch (Art. 21 DS-GVO)
- Recht, nicht einer automatisierten Einzelentscheidung unterworfen zu sein (Art. 22 DS-GVO)
- Recht auf Widerruf der Einwilligung (Art. 7 Abs. 2 DS-GVO)

Den Betroffenen steht das Recht zu, sich an eine Aufsichtsbehörde für Datenschutz wenden zu können. Die für die Max-Planck-Gesellschaft grundsätzlich zuständige Behörde ist das Bayerische Landesamt für Datenschutzaufsicht, Postfach 1349, 91504 Ansbach.

8. Grundsätze für die Verarbeitung von Beschäftigtendaten

8.1 Begriffsbestimmung

Beschäftigte der Max-Planck-Gesellschaft im datenschutzrechtlichen Sinn sind gemäß § 26 BDSG: Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeitnehmerinnen und Leiharbeitnehmer, zu ihrer Berufsbildung Beschäftigte, Stipendiatinnen und Stipendiaten, beamtenrechtsähnliche Anstellungsinhaber und Anstellungsinhaberinnen, Bewerberinnen und Bewerbers sowie Beschäftigte, deren Beschäftigungsverhältnis beendet ist, solange die Max-Planck-Gesellschaft deren personenbezogene Daten noch verarbeitet.

8.2 Rechtsgrundlagen

Personenbezogene Daten von Beschäftigten werden grundsätzlich insoweit verarbeitet, als sie für die Begründung, Durchführung und Beendigung der Beschäftigungsverhältnisse erforderlich sind oder vorrangige Rechtsvorschriften dies anordnen.

Soweit Kollektivvereinbarungen die Verarbeitung personenbezogener Daten regeln, gelten sie als Erlaubnisvorschrift auf der Grundlage von Art. 88 DS-GVO.

Weitere einzelfallbezogene Datenverarbeitungsprozesse werden – abgesehen von vorrangigen Rechtsvorschriften – auf Basis der Einwilligung oder des dokumentierten berechtigten Interesses, sofern die jeweiligen Voraussetzungen erfüllt sind, durchgeführt.

9. Grundsätze für die Verarbeitung von Daten in der Forschung

Die Max-Planck-Gesellschaft schützt die Rechte von Personen, die im Rahmen von Forschungsprojekten an Studien aktiv teilnehmen, die Teil von Beobachtungsstudien sind oder mit deren Daten oder Bioproben an den Max-Planck-Instituten geforscht wird. Dies gilt insbesondere, wenn es sich um schutzbedürftige Personen wie Minderjährige oder in ihrer Geschäftsfähigkeit eingeschränkte Personen handelt.

Forschung mit personenbezogenen Daten findet auf Basis der Einwilligung statt, wenn die Daten direkt bei den Teilnehmenden erhoben werden. Je nach Forschungsschwerpunkt kommt das Konzept des „Broad Consent“ unter Einhaltung der anerkannten ethischen Standards zur Anwendung. Sofern das Forschungsdesign keine aktive Teilnahme von Personen beinhaltet, erfolgt die Verarbeitung auf Basis des dokumentierten berechtigten Interesses unter Sicherstellung der angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte der betroffenen Personen.

Die Erfüllung der Betroffenenrechte, die Sicherstellung geeigneter technischer und organisatorischer Schutzmaßnahmen – die insbesondere auch aus Verträgen mit Dritten resultieren können – werden beim Studiendesign berücksichtigt und in der Projektbeschreibung dargestellt.

Die Max-Planck-Gesellschaft stellt für das Management von personenbezogenen Daten im Rahmen von Studienprojekten zwei selbst entwickelte Softwarelösungen zur Verfügung, die individuell von den Instituten genutzt bzw. in die vorhandene Infrastruktur integriert werden können.

10. Datenschutzmaßnahmen

10.1 Technische und organisatorische Maßnahmen (Art. 24, Art. 32 DS-GVO)

Die Max-Planck-Gesellschaft setzt ausgehend vom Schutzbedarf der personenbezogenen Daten und unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und um sicherzustellen, dass die Verarbeitung gemäß den gesetzlichen Vorgaben erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert. Personenbezogene Daten werden insbesondere vor versehentlicher oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder vor unbefugter Offenlegung von beziehungsweise unbefugtem Zugang zu personenbezogenen Daten geschützt.

10.2 Privacy by Design / Privacy by Default

IT-Systeme und Applikationen werden im Rahmen von Risikobetrachtungen grundsätzlich so ausgestaltet, dass sie die Vorgaben Datenschutz durch Technikgestaltung (privacy by design) und Datenschutz durch datenschutzfreundliche Voreinstellungen (privacy by default) des Art. 25 DS-GVO erfüllen.

10.3 Verpflichtung zur Vertraulichkeit

Alle Beschäftigten sowie externe Personen, die im Rahmen ihrer Tätigkeit Umgang mit personenbezogen Daten der Max-Planck-Gesellschaft haben, werden auf die Wahrung der Vertraulichkeit sowie die Einhaltung der externen und internen Regelungen verpflichtet.

10.4 Schulungen

Die Max-Planck-Gesellschaft verfügt über ein Schulungskonzept, das verpflichtende Basis-Schulungen für alle Beschäftigten sowie fachspezifische Schulungen enthält.

11. Verzeichnis von Verarbeitungstätigkeiten

Die Max-Planck-Gesellschaft führt ein zentrales Verzeichnis von Verarbeitungstätigkeiten, das alle Prozesse, in denen personenbezogene Daten verarbeitet werden, gemäß den Vorgaben des Art. 30 DS-GVO dokumentiert.

12. Datenschutz-Risikomanagement

Zur Beurteilung der mit der Verarbeitung personenbezogener Daten einhergehenden Risiken für die Rechte und Freiheiten der betroffenen Personen stellt die Max-Planck-Gesellschaft einen datenschutzspezifischen Leitfaden zur Risikobewertung bereit.

In Fällen, in denen eine Verarbeitung insbesondere aufgrund der Verwendung neuer Technologien voraussichtlich ein hohes Risiko für Betroffene zur Folge hat, wird anhand des Leitfadens eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchgeführt.

13. Umgang mit Meldepflichten

Die Prüfung von Meldepflichten im Fall von Verletzungen des Schutzes personenbezogener Daten nach Art. 33, 34 DS-GVO wird anhand eines vorgegebenen Verfahrens durchgeführt. Zeichnen sich aufgrund der an die Aufsichtsbehörde gemeldeten Fälle systemisch relevante Aspekte ab, werden diese an den Verwaltungsrat berichtet.

14. Zusammenarbeit mit Externen

Kommt es bei der Zusammenarbeit mit Externen zu einer Weitergabe personenbezogener Daten, wird geprüft, ob die speziellen Konstellationen der Auftragsverarbeitung (Art. 28 DS-GVO) oder Gemeinsamen Verantwortung (Art. 26 DS-GVO) vorliegen. Die Max-Planck-Gesellschaft hält hierfür jeweils Musterverträge vor.

DATA PROTECTION GUIDELINE of the Max-Planck-Gesellschaft

September 2021

ENGLISH VERSION

CONTENT

1. Objectives

The Max-Planck-Gesellschaft conducts basic research in the natural and biological sciences, the humanities and the social sciences for the benefit of society at large. Compliant handling of personal data forms a basis for a trusting relationship with study participants, employees, cooperation and business partners as well as all persons interested in research at the Max-Planck-Gesellschaft.

The Max-Planck-Gesellschaft takes into account the applicable data protection provisions in its strategic and operating decisions. In this, it takes appropriate account of the risks involved for the data subjects in the processing procedures.

2. Scope

This guideline is part of the data protection management system of the Max-Planck-Gesellschaft and describes the general principles for processing personal data and using data processing systems.

It is binding for all Institutes and facilities of Max-Planck-Gesellschaft e.V.[1] as well as for external parties involved as service providers or as users of data processing systems.

3. Legal requirements

The processing of personal data is bindingly governed by the EU General Data Protection Regulation (GDPR), the German Federal Data Protection Act (BDSG) as well as other national requirements. The regulations take precedence, if compliance with this guideline would result in a violation of these regulations.

4. Definition of terms

4.1 Personal data

Personal data within the meaning of Art. 4 no. 1 GDPR means all information which relates to an identified or identifiable natural person ("data subject"). A natural person is regarded as identifiable, if they can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person. The special categories of personal data according to Art. 9 para. [1] GDPR includes data revealing racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data concerning a natural person´s sex life or sexual orientation.

4.2 Processing

According to Art. 4 no. 2 GDPR, processing comprises any analogue or digital operation or set of operations relating to personal data, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

[1] The Max-Planck-Gesellschaft e.V. recommends that the legally independent institutions which are connected or associated with it should ensure a corresponding application and implementation of the Data Protection Guideline in their area of responsibility.

5. Responsibilities

The organizational structure of the Max-Planck-Gesellschaft under its Statutes involves various central and local function holders whose responsibilities include the implementation of the provisions of data protection law. The legal and statutory representatives of the Max-Planck-Gesellschaft e.V.[2] are legally responsible in external relationships. In this respect, they perform the function of the controllers according to the GDPR and BDSG. Internal responsibility is regulated in accordance with the Statutes of the Max-Planck-Gesellschaft. The Executive Committee is responsibility for supervision, whereas the managers of the facilities and Institutes are responsible for implementation. All employees must ensure within their respective areas of responsibility that the external and internal requirements are met when performing their activities. The Max-Planck-Gesellschaft is legally required to appoint a Data Protection Officer.

6. Principles for the processing of all personal data (Art. 5 GDPR)

6.1 Lawfulness

Personal data are processed lawfully and in good faith. Data are only processed, if this is required or explicitly permitted by the legal provisions of the GDPR, the BDSG or overriding legal provisions or if the data subject's consent has been obtained.

6.2 Purpose limitation

Personal data are processed only for legitimate purposes defined prior to data collection. Subsequent changes in the purposes of processing require a new review of an existing legal basis.

6.3 Transparency

The data subjects are informed of the respective data processing in accordance with the legal provisions. The information is provided in concise, transparent, comprehensible and easily accessible form using clear and plain language.

6.4 Data minimization

Any processing of personal data is designed to be limited, both quantitatively and qualitatively, to what is necessary for the purposes to be achieved. Where the purpose permits this and the expense is appropriate to the intended objective, anonymized data are used.

6.5 Accuracy

Personal data are processed accurate, completely and – where necessary – up to date. Appropriate measures are taken to ensure that incorrect, incomplete or outdated data are deleted, corrected, supplemented or updated.

6.6 Storage limitation

Personal data are generally only processed for as long as this is necessary to fulfill the respective purposes and no other legal, contractual or statutory retention periods apply.

[2] These are the Management Board according to § 26 BGB in conjunction with § 17 para. 1 of the Statutes of the Max-Planck-Gesellschaft and the Scientific Members with management function according to § 30 BGB, § 28 para. 3 of the Statutes.

6.7 Security of data processing

Personal data are protected against unauthorized access or disclosure, unlawful processing and accidental loss, alternation or destruction, using appropriate technical and organizational measures. These measures take into account the state of the art, the risks of the processing and the need for protection. The requirements for the measures are part of the information security management of the Max-Planck-Gesellschaft.

7. Ensuring the rights of the data subjects

All data subjects have the following rights under the legal provisions in relation to the Max-Planck-Gesellschaft:

- Right of access (Art. 15 GDPR)
- Right to rectification (Art. 16 GDPR)
- Right to erasure (Art. 17 GDPR)
- Right to restriction of processing (Art. 18 GDPR)
- Right to data portability (Art. 20 GDPR)
- Right to object (Art. 21 GDPR)
- Right not to be subjected to automated individual decision-making (Art. 22 GDPR)
- Right to withdrawal of consent (Art. 7 para. 2 GDPR)

The data subjects have the right to contact a supervisory authority for data protection. The authority generally responsible for the Max-Planck-Gesellschaft is the Bavarian State Office for Data Protection Supervision, PO Box 1349, 91504 Ansbach.

8. Principles relating to the processing of employee data

8.1 Definition of terms

Employees of the Max-Planck-Gesellschaft in the sense of data protection law are in accordance with § 26 BDSG: dependently employed workers including temporary workers, persons employed for occupational training purposes, scholarship holders, employees with a status similar to Civil Servants, applicants and employees whose relationship has ended as long as the Max-Planck-Gesellschaft still processes their personal data.

8.2 Legal bases

Personal data of employees are generally processed to the extent that is required in order to establish, implement and terminate the employment relationship or is required under overriding legal provisions.

Where the processing of personal data is governed by collective agreements, the latter are considered a permission provision based on Art. 88 GDPR.

Other individual case-related data processing operations are carried out — apart from overriding legal provisions — on the basis of consent or documented legitimate interest, provided that the respective requirements are met.

9. Principles relating to the processing of data in research

The Max-Planck-Gesellschaft protects the rights of persons who actively participate in studies as part of research projects, who take part in observational studies or whose data or biosamples are used for research at the Max Planck Institutes. This applies especially where vulnerable persons such as minors or persons who are limited in their legal capacity are involved.

Research involving personal data takes place based on consent, if the data are collected directly from the participants. Depending on the research focus, the concept of "broad consent" is applied, in compliance with the recognized ethical standards. Where the research design does not involve the active participation of persons, the processing is based on documented legitimate interest while ensuring appropriate and specific measures to protect the rights of the data subjects.

The fulfillment of data subjects' rights, the securing of appropriate technical and organizational protection measures — which may result in particular from contracts with third parties — are taken into account in the study design and presented in the project description.

The Max-Planck-Gesellschaft provides two internally developed software solutions for managing personal data in the context of study projects which can be used individually by the Institutes or integrated into the existing infrastructure.

10. Data protection measures

10.1 Technical and organizational measures (Art. 24, Art. 32 GDPR)

The Max-Planck-Gesellschaft implements suitable technical and organizational measures based on the need for protection of the personal data and taking into account the nature, scope, circumstances and purpose of the processing as well as the risk of varying likelihood and severity for the rights and freedom of natural persons in order to ensure a protection level that is appropriate for the risk and to make sure that the processing is in accordance with the legal requirements. These measures are reviewed and updated, where necessary. Personal data are particularly protected against unintentional or unlawful destruction, loss, change or unauthorized disclosure of or unauthorized access to personal data.

10.2 Privacy by Design / Privacy by Default

IT systems and applications are generally designed in the context of risk assessments in such a way that they meet the requirements of Article 25 of the GDPR for technical design (privacy by design) and for data-protection-friendly defaults (privacy by default).

10.3 Obligation of confidentiality

All employees and external persons who come into contact with personal data of the Max-Planck-Gesellschaft as part of their activity are obligated to maintain confidentiality and comply with the internal and external regulations.

10.4 Training

The Max-Planck-Gesellschaft has a training concept which contains mandatory basic training for all employees as well as subject-specific training.

11. Record of processing activities

The Max-Planck-Gesellschaft maintains a central record of processing activities which documents all processes in which personal data are processed in accordance with the requirements of Art. 30 GDPR.

12. Data protection risk management

In order to assess the risks involved in the processing of personal data for the rights and freedom of the data subjects, the Max-Planck-Gesellschaft provides a risk assessment guideline specifically for data protection.

In cases where the processing is likely to result in high risk for the data subjects, in particular due to the use of new technologies, a data protection impact assessment pursuant to Article 35 of the GDPR is carried out using the guideline.

13. Handling of notification obligations

The verification of notification obligations in case of personal data breaches according to Art. 33, 34 GDPR is carried out using a prescribed procedure. If systematically relevant aspects become apparent based on the cases reported to the supervisory authority, these are reported to the Executive Committee.

14. Collaboration with external parties

If personal data are transferred during a collaboration with external parties, a review must be carried out to determine whether the specific constellations of processing on behalf (Art. 28 GDPR) or of joint controllers (Art. 26 GDPR) apply. The Max-Planck-Gesellschaft maintains sample contracts for such situations.

HERAUSGEBER
Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
Hofgartenstr. 8, 80539 München
E-Mail: datenschutz@mpg.de

PUBLISHER
Max Planck Society for the Advancement of Science
Hofgartenstr. 8, 80539 München
Email: datenschutz@mpg.de