Wir stärken, schützen, fördern.

Unsere Einrichtungen bieten dafür den Rahmen.

Datenschutzrichtlinien

Elterninitiative Pliening e.V
im Plieninger Familienland

Datenschutz ist für uns mehr als eine rechtliche Angelegenheit. Es ist auch eine Frage des gegenseitigen Vertrauens und der Achtung der Persönlichkeitsrechte jedes Einzelnen.

Elterninitiative Pliening e.V
Kirchweg 31
85652 Pliening
Tel. 08121 22309-10
kontakt@eip-pliening.de
www.eip-pliening.de

Stand: Mai 2018

Inhalt

Vorwort 3

A. Grundsätze der Datenverarbeitung 3

1. Allgemeines 3
   1.1. Einhaltung der Rechtsvorschriften 3
   1.2. Geltungsbereich 3
   1.3. Verantwortlichkeiten 3
   1.4. Schulung 3

2. Grundlagen der Datenverarbeitung 4
   2.1. Was bedeutet für uns Datenverarbeitung 4
   2.2. Wofür verarbeiten wir personenbezogene Daten 4
   2.3. Wann ist Datenverarbeitung zulässig 4

3. Prinzipien für die Verarbeitung personenbezogener Daten 5
   3.1. Fairness und Rechtmäßigkeit 5
   3.2. Zweckbindung 5
   3.3. Transparenz 5
   3.4. Datenvermeidung und Datensparsamkeit 5
   3.5. Vertraulichkeit und Richtigkeit der Daten 5
   3.6. Sichere Datenübermittlung 5
   3.7. Recht auf Vergessen 5

B. Regeln für den Umgang mit personenbezogenen Daten 6

1. Umgang mit Daten im Alltag 6
   1.1. Berechtigte Personen 6
   1.2. Datensicherheit am Arbeitsplatz 6
   1.3. Keine Daten verlassen das Haus 6
   1.4. Daten vernichten und löschen 6
   1.5. Datensicherheit in Portfolios 6
   1.6. Wahrung von Schweigepflicht und Datengeheimnis 6

2. Elektronische Datenverarbeitung 7
   2.1. Allgemeine Regelungen 7
   2.2. Arbeitsplatz 7
   2.3. Passwort-Gebrauch 7
   2.4. Schutz vor Schad-Inhalten 7
   2.5. Schutz vor unverlangter Werbung („Spam“) 7
   2.6. Nutzung von E-Mail/Internet 8

3. Datenschutzvorfälle 8

C. Inkraftsetzung 8

Vorwort

Die Elterninitiative Pliening e.V. (EIP) ist ein gemeinnütziger Verein, der die Interessen der Familien mit Kindern aller Altersstufen aus der Gemeinde Pliening und angrenzender Gemeinden vertritt, insbesondere durch Betreuung und Förderung von Kindern, Jugendlichen und Familien. Um die vielfältigen Aufgaben und Angebote ausführen zu können, ist es notwendig, dass personenbezogene Daten erhoben, verarbeitet und genutzt werden. Dabei nehmen wir den Schutz dieser Daten sehr ernst und haben dies auch entsprechend organisiert.

Die EIP verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung des gesetzlichen Datenschutzrechtes.

Die Wahrung des Datenschutzes ist die Basis für eine vertrauensvolle Zusammenarbeit mit unseren Mitgliedern, Mitarbeitern/innen und Kunden.

Mit dieser Leitlinie zum Datenschutz und zur IT-Sicherheit setzt die EIP den Rahmen für den Umgang mit personenbezogenen Daten für alle Bereiche des Vereins.

A. Grundsätze der Datenverarbeitung

1. Allgemeines

1.1. Einhaltung der Rechtsvorschriften

Die Rechtsgrundlage für die Erhebung personenbezogener Daten ergibt sich aus Art. 6 – 11 der DSGVO. Bei der Benutzung der IT-Systeme der EIP sind von den Mitarbeitern/innen die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die internen Regelungen einzuhalten. Bei Unsicherheiten wenden sich die Mitarbeiter/innen zur Klärung an ihre Vorgesetzten.

1.2. Geltungsbereich

Diese Datenschutzrichtlinie hat für alle haupt- und ehrenamtlich Beschäftigen der Elterninitiative Pliening e.V. Gültigkeit. Vorstände, Geschäftsführung und alle Mitarbeiter/innen sind sich ihrer Verantwortung für die Informations- und Datensicherheit bewusst. Auch externe Personen, die regelmäßig bei uns tätig sind, sind verpflichtet, sich an diese Richtlinie zu halten.

1.3. Verantwortlichkeiten

Die **Hauptverantwortung für die Einhaltung des Datenschutzes** tragen die Vorsitzenden der Elterninitiative Pliening e.V.

Für **Aufbau und Umsetzung eines effektiven Datenschutzmanagements** ist die Geschäftsführung verantwortlich. Sie hat sicherzustellen, dass die gesetzlichen Vorgaben und die Regelungen der Datenschutzrichtlinie eingehalten werden.

Für die Einhaltung der **Regeln bei Verarbeitung von und Umgang** mit personenbezogenen Daten ist jede/r Mitarbeiter/in am eigenen Arbeitsplatz verantwortlich.

1.4. Schulung

Die Geschäftsführung muss sicherstellen, dass alle Mitarbeiter/innen im erforderlichen Umfang zum Datenschutz geschult werden und die erforderlichen Anweisungen erhalten.

2. Grundlagen der Datenverarbeitung

2.1. Was bedeutet für uns Datenverarbeitung

Personenbezogene Daten sind alle Angaben, die sich **Personen zuordnen lassen**. Dazu gehören nicht nur Name und Anschrift, sondern auch Beobachtungen, die in Berichten festgehalten werden. Auch Aufzeichnungen mit wertenden Aussagen (z. B. zu Lernleistungen oder soziale Fähigkeiten) sowie Foto- oder Filmaufzeichnungen sind personenbezogene Daten.

Datenverarbeitung geschieht auf verschiedene Weise:

Erheben: das Beschaffen von Daten über den Betroffenen
Verarbeiten: das **Speichern, Verändern, Übermitteln, Sperren** oder **Löschen** von Daten
Nutzen: jede Verwendung der Daten, die nicht *Erheben* oder *Verarbeiten* ist

Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit eine **Rechtsvorschrift** dies erlaubt oder anordnet oder die **Einwilligung** des Betroffenen vorliegt.
Wichtig: Personenbezogene Daten sind grundsätzlich nur bei der betroffenen Person zu erheben.

2.2. Wofür verarbeiten wir personenbezogene Daten

- zur Organisation des Betriebes (Name, Adresse, ….)
- zur Finanzierung der Kinderbetreuung (Bankverbindung)
- für die pädagogische Arbeit nach BayKiBiG und BEP (Informationen zum Kind und Familie)
- Zur Wahrung rechtlicher Vorschriften (Vorsorgeuntersuchung, Migration, Behinderung,….)
- Zur individuellen Wohl des Kindes (Allergien, Medikamente,….)
- Zur Durchführung von Kursen und Veranstaltungen

2.3. Wann ist Datenverarbeitung zulässig

Datenverarbeitung aufgrund einer vertraglichen Beziehung
Wenn die Datenverarbeitung zur Vertragserfüllung (Betreuungsvertrag, Mitgliedsvertrag, Arbeitsvertrag, usw.) dient, so ist die Verarbeitung zulässig.

Datenverarbeitung aufgrund von Einwilligungserklärung
Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor einer Einwilligung muss der Betroffene informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischem Kontakt, kann die Einwilligung auch mündlich erteilt werden. Dies muss dokumentiert werden.

Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten (z.B. BayKiBiG).

Datenverarbeitung aufgrund berechtigten Interesses
Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses erforderlich ist. Berechtigte Interessen bestehen in der Regel bei rechtlichen (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftlichen Themen.

Nutzerdaten und Internet
Voraussetzung für die Nutzung der personenbezogenen Daten, die auf unserer Webseite erhoben werden, ist die Datenschutzerklärung und der Hinweis auf die Verwendung von Cookies.

https://www.eip-pliening.de/allgemeines/impressum.htmlImpressum

3. Prinzipien für die Verarbeitung personenbezogener Daten

3.1. Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten achten wir auf das informationelle Selbstbestimmungsrecht des Betroffenen. Personenbezogene Daten werden nur auf rechtmäßige Weise erhoben und verarbeitet. Wo erforderlich, werden schriftliche Einwilligungserklärungen eingeholt.

3.2. Zweckbindung

Wenn personenbezogenen Daten erhoben werden, muss der Zweck der Erhebung erkenntlich sein. Zu einem anderen Zweck werden die Daten ohne weitere Einwilligung nicht verwendet.

3.3. Transparenz

Die Betroffenen müssen über den Umgang mit ihren Daten informiert werden. Grundsätzlich sind die Daten bei den Betroffenen direkt zu erheben. Bei der Erhebung der Daten müssen die Betroffenen erkennen können oder entsprechend informiert werden über

- den Zweck der Datenverarbeitung,
- die hinterlegten Aufbewahrungsfristen und
- an wen die Daten gegebenenfalls übermittelt werden

3.4. Datenvermeidung und Datensparsamkeit

Wir erheben nur Daten, die unbedingt erforderlich sind um den angestrebten Zweck zu erreichen. Wir speichern keine personenbezogenen Daten auf Vorrat für zukünftige Zwecke, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

3.5. Vertraulichkeit und Richtigkeit der Daten

Wir gehen mit den erhobenen Daten sorgfältig und vertraulich um und achten darauf, dass die Daten richtig erhoben und richtig gespeichert werden.

3.6. Sichere Datenübermittlung

Die Übermittlung von personenbezogenen Daten an Empfänger außerhalb der EIP geschieht nur zur Einhaltung gesetzlicher Vorschriften oder wenn eine Einwilligungserklärung vorliegt. Wir achten auf sichere Übermittlung der Daten.

3.7. Recht auf Vergessen

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, werden gelöscht bzw. sicher vernichtet. Liegt keine Aufbewahrungsfrist vor, werden die Daten bei Beendigung des Zweckes für die sie erhoben werden gelöscht. Genauso verfahren wir auch bei Widerruf.

B. Regeln für den Umgang mit personenbezogenen Daten

1. Umgang mit Daten im Alltag

1.1. Berechtigte Personen

Personenbezogene Daten dürfen nur von Mitarbeiter/innen erhoben und verarbeitet werden, die damit im Rahmen ihrer Aufgaben betraut und berechtigt sind. Dies sind in der Regel die Leitungen der Einrichtungen und die Mitarbeiter/innen in der Verwaltung. Zugang zu personenbezogenen Daten erhalten Mitarbeiter/innen in dem Umfang, wie dies für die jeweiligen Aufgaben erforderlich ist. (Kinderlisten, Kurslisten,...)

1.2. Datensicherheit am Arbeitsplatz

Akten, Dokumente und Notizen mit personenbezogenen Daten dürfen beim Verlassen des Arbeitsplatzes nicht offen liegen bleiben. Das Büro muss abgeschlossen werden, wenn niemand dort arbeitet. Schränke, in denen sich personenbezogene Daten befinden, müssen außerhalb der Dienstzeiten verschlossen sein.

Damit Unbefugte keine Einsicht in personenbezogene Daten erhalten können, dürfen keine Listen, Datenblätter, etc. am Arbeitsplatz offen liegen gelassen werden.

1.3. Keine Daten verlassen das Haus

Unterlagen mit personenbezogenen Daten dürfen grundsätzlich nur mit Einwilligung der Leitung die Einrichtung verlassen. Es ist unzulässig, im privaten Bereich personenbezogene Daten, Berichte, Fotos, usw. aus der Arbeit aufzubewahren.

Informationen und Daten (auch Fotos) aus dem beruflichen Alltag dürfen nicht über soziale Netzwerke ausgetauscht werden.

Ein Verlust oder eine Veröffentlichung von geschützten Daten in jeglicher Form außerhalb der Dienststelle kann für Mitarbeiter/innen arbeits-, zivil- und strafrechtliche Folgen haben.

1.4. Daten vernichten und löschen

Papiere mit personenbezogenen Daten die nicht mehr benötigt werden und bei denen keine Aufbewahrungspflicht besteht, müssen, sicher vernichtet werden (Shreddern). Elektronisch gespeicherte Daten, auch Mails und Faxe, müssen ebenfalls vollständig und sicher gelöscht werden.

1.5. Datensicherheit in Portfolios

Portfolios müssen nicht verschlossen aufbewahrt werden. Es muss aber gewährleistet werden, dass die Kinder, bzw. deren Eltern nur die eigenen Unterlagen einsehen. Unterlagen anderer Kinder dürfen nur mit Einwilligung des jeweiligen Kindes eingesehen werden. In Portfolios werden keine sensiblen Daten zum Kind abgelegt. (keine Entwickelungsberichte, usw.) Bei Austritt des Kindes wird das Portfolio an die Eltern, bzw. das Kind übergeben.

1.6. Wahrung von Schweigepflicht und Datengeheimnis

Alle Angestellten müssen sich mit Unterschrift zur Einhaltung von Schweigepflicht und zur Wahrung des Datengeheimnisses verpflichten und werden entsprechend belehrt.

2. Elektronische Datenverarbeitung

2.1. Allgemeine Regelungen

Die Nutzung der IT-Systeme ist ausschließlich zu dienstlichen Zwecken und im jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der ausdrücklichen Erlaubnis des Arbeitgebers.

Daten in elektronischer Form werden nur auf dem Server der EIP gespeichert. Es dürfen keine Daten auf externe Datenträger oder private PCs übertragen werden.

Der Zugang zum Arbeitsplatz muss mit Passwort gesichert sein.

2.2. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen des Arbeitsplatzes grundsätzlich zu verschließen. Bei zwischenzeitlichem Weggang vom PC muss der Arbeitsplatz vom Server getrennt werden, so dass vor der erneuten Nutzung eine Authentifizierung erforderlich wird. Dies ist auf einfache Weise mit der Tastenkombination Windows + l möglich.

Für den Homeoffice-Arbeitsplatz gelten die gleichen Regeln. Mitarbeiter/innen, die mittels VPN-Zugang arbeiten, müssen gewährleisten, dass keine anderen Personen als sie selbst Einblick und Zugang zu den Daten haben können.

2.3. Passwort-Gebrauch

Das IT-System der EIP ist so gestaltet, dass ein Zugang nur mit Passwort möglich ist. Die Authentifizierung erfolgt durch die Verwendung der Kombination Benutzername/Passwort. Jeder/m berechtigten Mitarbeiter/in wird ein eigenes Passwort zugewiesen und ist dafür verantwortlich. Das zugeteilte Passwort muss nach Zuteilung sofort geändert werden.

Das Passwort ist so zu wählen, dass es sicher ist. Es sollte mindestens 8 Zeichen haben und Zahlen und Sonderzeichen beinhalten. Vor-und Familiennamen oder Geburtstage sowie Namen von Angehörigen sind nicht als Passwort geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter müssen regelmäßig geändert werden. Bereits genutzte Passwörter dürfen nicht noch einmal wieder verwendet werden.

2.4. Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutz-programme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen.

Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist dies der Verwaltung zu melden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Absprache mit der IT-Beratung geöffnet werden.

2.5. Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung durch E-Mail werden so genannte Spam-Filter eingesetzt. Durch den Spam-Filter kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt werden oder im Spamordner gespeichert sind. Dies kann bei erwünschten Mail vermieden werden, indem die erwünschten Absender in das Mail-Adressbuch eingetragen werden.

2.6. Nutzung von E-Mail/Internet

Soweit nicht ausdrücklich eine Zustimmung erfolgt ist, darf die Nutzung von E-Mail und Internet nur für dienstliche Zwecke erfolgen.

Geschützte Daten müssen bei einer notwendigen Übermittlung per Email verschlüsselt werden. **Vorsicht:** die Verteilerliste in Emails enthält auch geschützte Daten in Form von persönlichen Emailadressen. Diese müssen geschützt werden, indem sie unter „Bcc" eingegeben werden, da sie dann für die Empfänger nicht mehr sichtbar werden.

Die Weitergabe von dienstlichen Informationen oder Bildern über soziale Netzwerke ist grundsätzlich verboten. (Verstoß gegen Schweigepflicht). Solche Daten entziehen sich der Kontrolle, eine nachträgliche Löschung ist normalerweise nahezu unmöglich.

3. Datenschutzvorfälle

Jede/r Mitarbeiter/in muss der Geschäftsleitung unverzüglich melden, wenn der Schutz oder die Sicherheit von personenbezogenen Daten in irgendeiner Weise gefährdet ist oder wenn gegen diese Richtlinien und andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle) verstoßen worden ist.

Dies ist u.a. auch notwendig, da in Fällen von
- unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten (z.B. Einbruch), oder
- Verlust personenbezogener Daten

die staatlichen Meldepflichten von Datenschutzvorfällen erfüllt werden müssen.

Durch organisatorische, personelle und technische Maßnahmen ist eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.

C. Inkraftsetzung

Die Richtlinien zum Datenschutz haben ab sofort Gültigkeit. Sie werden regelmäßig sowie bei Bedarf auf Vollständigkeit und Aktualität überprüft. Änderungen dieses Dokuments liegen in der Verantwortung der Geschäftsführung.
Diese Richtlinien sind allen Mitarbeitern/innen bekannt zu geben und zugänglich zu machen.

Pliening, den 26.06.2018

Geschäftsführung Elterninitiative Pliening e.V.

Ergänzende Unterlagen
Belehrung zum Datenschutz
Information zur Datenerhebung im Arbeitsverhältnis
Erklärung der Mitarbeiter/innen zur Einhaltung des Datenschutzes
Verzeichnis der Verarbeitungstätigkeiten
Dokumentation der technisch-organisatorischen Maßnahmen (TOM)
u.a.