Anlage 2

# Verzeichnis der Auftragsverarbeiter

--- Stand: 23. Mai 2024 ---

Vertragsverhältnisse, bei denen der Auftragnehmer die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Auftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat der Auftragsverarbeiter sicherzustellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

Alle Daten, die durch phase6 oder Auftragsverarbeiter verarbeitet werden, werden **regelmäßig und systematisch nur im Rechtsraum der DSGVO verarbeitet.** Sofern nachfolgend vom **Europäischen Wirtschaftsraum (EWR)** die Rede ist, ist damit **stets der Rechtsraum der DSGVO gemeint.** Die Rechtsgrundlage der Verarbeitung basiert auf Verträgen mit unseren Auftragsverarbeitern. Details sind der nachfolgenden Tabelle zu entnehmen.

## Liste der Auftragsverarbeiter / externe Empfänger von Daten

| Auftrags-verarbeiter | Unterauftrags-verarbeiter | Firmen-hauptsitz | Daten-residenz | Zweck der Verarbeitung | PII? | Speicher-dauer |
|---|---|---|---|---|---|---|
| **Datenresidenz**: Vom Auftragsverarbeiter vertraglich zugesicherter Standort der Datenverarbeitung.<br>**PII**: Daten, die dem Auftragsverarbeiter die Rückverfolgung oder Identifikation einer Person ermöglichen.<br>phase6 versichert, dass die Datenresidenz und die dort verarbeiteten Daten im Rahmen eines Prüfprozesses kontrolliert und abgenommen worden sind. | | | | | | |
| Hetzner Online GmbH (DPA) | - | DE | DE | Betrieb der Serversysteme zur Erbringung der Lern-angebote, Hostingdaten | JA | 90 Tage bis dauerhaft |
| Horizon Alpha GmbH & Co KG (DPA) | - | DE | - | Dienstleistungen im Bereich der Entwicklung | JA | 30 Tage |
| Igor Dobrovolskyi (SCCs[2]) | - | UA | - | Dienstleistungen im Bereich der Entwicklung | JA[1] | 1 Woche |
| Intellias Global Limited (DPA/SCC[2]) | TzOV IIT Intellas (UA), TzOV Intellias Consulting (UA) | MT | - | Dienstleistungen im Bereich der Entwicklung und Qualitätssicherung | JA[1] | 1 Woche |

## Optionale Auftragsverarbeiter

Die Datenverarbeitung über die folgenden Auftragsverarbeiter ist optional und kann insbesondere für die schulische Nutzung per Voreinstellung deaktiviert werden. Die gewünschte Verarbeitung wird bei Vertragsschluss entweder im Hauptvertrag (siehe “Strikter Modus”) oder in Anlage 3 geregelt. Darüber hinaus kann eine Einschränkung der Verarbeitung jederzeit nachträglich formlos per E-Mail an datenschutz@phase-6.de beantragt werden.

| Auftrags-verarbeiter | Unterauftrags-verarbeiter | Firmen-hauptsitz | Daten-residenz | Zweck der Verarbeitung | PII? | Speicher-dauer |
|---|---|---|---|---|---|---|
| **Datenresidenz**: Vom Auftragsverarbeiter vertraglich zugesicherter Standort der Datenverarbeitung.<br>**PII**: Daten, die dem Auftragsverarbeiter die Rückverfolgung oder Identifikation einer Person ermöglichen.<br>phase6 versichert, dass die Datenresidenz und die dort verarbeiteten Daten im Rahmen eines Prüfprozesses kontrolliert und abgenommen worden sind. | | | | | | |
| Adjust GmbH (DPA) | Leaseweb Germany GmbH | DE | EWR | Erfolgsmessung von Werbekampagnen in den App Stores. | NEIN | Dauerhaft |
| Amazon AWS (DPA/SCCs) | A100 ROW GmbH | USA | DE | Verwendete Dienste: Amazon SES zum Versand von E-Mails | JA | KEINE |
| Amplitude Inc. (DPA/SCCs) | Amazon AWS Devo Technology Inc. | USA | DE | Amplitude erfasst Daten zum Zweck der weiteren Produktverbesserung. | NEIN | Dauerhaft |
| Google LLC (DPA/SCCs) | Firebase, Inc Google Cloud Platform | USA | EWR | Absturzberichte, Steuerung des App Verhaltens, Problemerkennung nach App-Updates, Push-Benachrichtigungen, Erfolgsmessung von Werbekampagnen in Suchmaschinen und Apps, App-Links | NEIN | 14 Monate |
| Mouseflow ApS | LeaseWeb Netherlands B.V. | DK | EWR | Stichprobenhafte Aufzeichnung einer Browser-Sitzung zum Zwecke der Problemanalyse, bei der personenbezogene Daten automatisch maskiert werden. | NEIN | 90 Tage |
| Scaleway S.A.S. (DPA) | * | FR | NL, FR, PL | Betrieb der Serversysteme zur Erbringung des Angebots von Planet Pop | JA | Dauerhaft |
| Survicate Sp. Z O. O. | Amazon AWS | PL | IE (Irland) | Interaktive Umfragen | NEIN | Dauerhaft |

*Aktuelle Liste der Unterauftragsverarbeiter: https://www.scaleway.com/en/subprocessorlist/

# Datenschutzbezogene Einschätzung

Die Datenschutzbezogene Einschätzung befasst sich nachfolgend mit Auftragsverarbeitern oder Unterauftragsverarbeitern, die Verflechtungen außerhalb des EWR haben oder bei denen persönlich identifizierbare Informationen (PII) verarbeitet werden.
Es werden keine besonders sensiblen personenbezogenen Daten verarbeitet. (Art 35 DSGVO)

**Adjust GmbH:** phase6 stellt durch vertragliche Maßnahmen, technische Konfiguration und anlassbezogene als auch regelmäßige jährliche Prüfung der Daten sicher, dass nur die vertraglich zugesicherten Datenkategorien erfasst und innerhalb des EWR verarbeitet werden.

**Amazon AWS**: phase6 stellt durch vertragliche Maßnahmen und technische Konfiguration sicher, dass die über Amazon SES verarbeiteten personenbezogenen Daten nur zweckgebunden verarbeitet und nicht gespeichert werden. Der Dienst von Amazon wird nur zur Übermittlung und nicht zum Empfang von E-Mails verwendet. Log-Dateien enthalten weder die E-Mail-Adresse des Empfängers noch den Inhalt der übermittelten E-Mail. phase6 wird anhand einer “Message ID” von Amazon informiert, sofern es zu Problemen bei der Zustellung oder Beschwerden kommt. Das Zustell- und Beschwerde-Management läuft über die selbstverwalteten Server bei der Hetzner Online GmbH, so dass keine E-Mail-Adressdaten bei Amazon gespeichert werden.

**Amplitude Inc.**: phase6 stellt durch vertragliche Maßnahmen, technische Konfiguration und anlassbezogene als auch regelmäßige jährliche Prüfung der Daten sicher, dass die durch Amplitude verarbeiteten Datenkategorien der Dokumentation entsprechen, keine PII enthalten und systematisch und regelmäßig nur innerhalb des EWR verarbeitet werden. Detaillierte Informationen zur vertraglichen Ausgestaltung und der verarbeiteten Daten befinden sich in Anhang 1.

**Google LLC**: phase6 stellt durch vertragliche Maßnahmen, technische Konfiguration und anlassbezogene als auch regelmäßige jährliche Prüfung der Daten sicher, dass die durch Google verarbeiteten Datenkategorien der Dokumentation entsprechen, keine PII enthalten und nur innerhalb des EWR verarbeitet werden. Detaillierte Informationen zu den verarbeiteten Daten befinden sich in Anhang 2.

**Horizon Alpha GmbH & Co KG:** phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden.

**Hetzner Online GmbH**: phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden.

**Igor Dobrovolskyi**: Partner hat alle datenschutzrelevanten Prozesse der phase6 in Zusammenarbeit mit dem Datenschutzbeauftragten umgesetzt. Er ist in besonderem Maße fachkundig im Umgang mit PII und arbeitet seit ca. 20 Jahren ausschließlich für phase6. Im Vertrag mit dem Auftragsverarbeiter ist ausdrücklich geregelt, dass personenbezogene Daten lediglich im Einzelauftrag verarbeitet werden dürfen und dass die Verarbeitung auf den Servern der Hetzner Online GmbH stattfindet. Ebenfalls ist ausdrücklich geregelt, dass, falls Daten im Einzelauftrag zur Analyse heruntergeladen werden müssen, diese unmittelbar nach Bearbeitung des Anliegens wieder gelöscht werden. Weitere Informationen siehe “**Datenübertragung in Drittländer / Ukraine (TIA)**”

**Intellias Global Limited**: Partner ist ISO/IEC 27001:2013 zertifiziert:
CSR Report: https://www.intellias.com/corporate-social-responsibility/
ISO/IEC 27001:2013: https://intellias.com/intellias-earns-iso-iec-27001-2013-certification/
Eine Zusammenarbeit mit phase6 besteht seit mehr als 10 Jahren. Alle Mitarbeiter sind gut geschult und arbeiten ausschließlich für phase6. Im Vertrag mit dem Auftragsverarbeiter ist ausdrücklich geregelt, dass personenbezogene Daten lediglich im Einzelauftrag verarbeitet werden dürfen und dass die Verarbeitung auf den Servern der Hetzner Online GmbH stattfindet. Ebenfalls ist ausdrücklich geregelt, dass, falls Daten im Einzelauftrag zur Analyse heruntergeladen werden müssen, diese unmittelbar nach Bearbeitung des Anliegens wieder gelöscht werden. Weitere Informationen siehe “**Datenübertragung in Drittländer / Ukraine (TIA)**”

**Mouseflow ApS**: Der Dienst erlaubt die stichprobenhafte Aufzeichnung einer Browser-Sitzung zum Zwecke der Problemanalyse. Dies ist vor allem für den Kundensupport oder die Produktentwicklung hilfreich, um besser verstehen zu können, warum ein Nutzer die Lernapps nicht wie erwartet nutzen kann. phase6 hat ausgiebig kontrolliert, dass alle potentiell in der Aufzeichnung zu sehenden direkten personenbezogenen Daten erfolgreich maskiert werden. Über Mouseflow aufgezeichnete Videos werden nach maximal 90 Tagen gelöscht.

**Scaleway S.A.S.**: phase6 stellt sicher, dass keine Daten außerhalb des EWR verarbeitet werden. Zwar nutzt Scaleway insbesondere im Marketing und im Support auch Unterauftragsverarbeiter in unsicheren Drittländern, dies ist aber im Kontext von phase6 nicht der Fall. Scaleway hat uns auf Anfrage bestätigt, dass die als "Processor" verarbeiteten Daten (alle Daten, die phase6 im Konto hochlädt) nur in eigenen europäischen Rechenzentren oder mit europäischen Diensten gespeichert oder verarbeitet werden.

**Survicate Sp. Z O. O.**: Der Dienst erlaubt die Durchführung interaktiver Umfragen zum Zwecke der Problemanalyse. Dies ist vor allem für die Produktentwicklung hilfreich, um das Angebot für den Kunden zu verbessern. Die über Survicate verarbeiteten Daten erhalten keine PII.

## Datenübertragung in Drittländer / Ukraine (TIA)

Überprüfung der Zulässigkeit einer Datenübertragung in ein Drittland anhand der Prüfschablone des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Pruefschritte_Datenuebermittlung_in_Drittlaender_nach_Schrems_II.pdf

(1) Es erfolgt eine Datenübertragung in ein Drittland (=Ukraine). Es erfolgt keine regelmäßige oder systematische Verarbeitung personenbezogener Daten. Ein Zugriff erfolgt nur im Einzelfall, wenn dies zur Erbringung unserer Leistungen erforderlich ist (bspw.bei der Erstellung eines Support-Tickets, für deren Bearbeitung eine technische Überprüfung notwendig ist). Die Verarbeitung erfolgt stets auf den Servern der Hetzner Online GmbH über eine verschlüsselte und sichere Verbindung. Sollten zur Fehleranalyse tatsächlich Daten übertragen werden, werden diese Daten nach der Bearbeitung gelöscht. **Der Anteil der Daten, die auf diese Weise überprüft werden, liegt vertraglich zugesichert bei deutlich unter einem Prozent der jährlich aktiv lernenden Nutzer von phase6**.

Rechtsvorschriften und Gepflogenheiten in der Ukraine (zuletzt aktualisiert am 05.07.2023):

Gesetz der Ukraine über den Schutz personenbezogener Daten (aktuelle Fassung - Revision am 27.10.2022):
https://zakon.rada.gov.ua/laws/show/2297-17?lang=en#Text
Gesetz der Ukraine über Information (aktuelle Fassung - Revision am 21.03.2023):
https://zakon.rada.gov.ua/laws/show/2657-12?lang=en#Text
Verordnung über die Genehmigung von Dokumenten auf dem Gebiet des Schutzes personenbezogener Daten (aktuelle Fassung, 08.01.2014):
https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

Die Ukraine hat die Datenschutzgrundverordnung (GDPR) nicht als eigene Gesetzgebung übernommen. Das ukrainische Gesetz über den Schutz personenbezogener Daten stimmt jedoch mit bestimmten Grundsätzen und Konzepten der Datenschutzgrundverordnung überein. Das ukrainische Gesetz enthält Bestimmungen zu den Rechten der betroffenen Personen, zu den Pflichten der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter, zu den Zustimmungserfordernissen und zu Sicherheitsmaßnahmen.

Es gibt einen bevollmächtigten Menschenrechtsbeauftragten des ukrainischen Parlaments für den Bereich des Schutzes personenbezogener Daten.

Die ukrainischen Datenschutzgesetze und -vorschriften beeinträchtigen die Einhaltung der EU GDPR-Anforderungen durch unsere Auftragsverarbeiter nicht.

(2) Weitere Maßnahmen, nach “Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten” des European Data Protection Boards, insbesondere Punkt 135-137 (https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf):

Verhaltenskodizes und internationale Standards:

Intellias ist ISO 27001 zertifiziert. Alle Büros in der Ukraine sind in der Zertifizierung eingeschlossen und werden regelmäßig sowohl intern als auch extern überprüft. Im Jahr 2023 hat Intellias das Rezertifizierungsaudit erfolgreich bestanden.

Gleichzeitig ist Intelias ein TISAX-zertifiziertes Unternehmen.
(TISAX ist eine Bewertung der Informationssicherheit in der europäischen Automobilindustrie).

Die Informationssicherheitsgruppe bei Intellias besteht aus:
Manager für Informationssicherheit, Analyst für Informationssicherheit, Ingenieur für Informationssicherheit, Architekt für Informationssicherheit, Ingenieur für den Betrieb der Informationssicherheit. Die internen Prüfer von Intellias sind ebenfalls nach ISO 27001 zertifiziert. Die Infrastruktur von Intellias wird regelmäßig von der Informationssicherheitsgruppe auf Schwachstellen untersucht.

Die Intellias-Büros in der Ukraine sind mit Zugangskontrollsystemen, Videoüberwachung und Sicherheitsalarmen ausgestattet und werden durch Sicherheitspersonal geschützt.

Es wurde ein umfassender Betriebskontinuitätsplan entwickelt, der regelmäßig überprüft wird.

Alle Intellias-Büros sind an mindestens drei Internet-Provider und eine Satelliten-Breitbandinternetverbindung angeschlossen und mit Stromgeneratoren ausgestattet.

Alle Intellias-Mitarbeiter unterzeichnen eine Geheimhaltungsverpflichtung und nehmen an obligatorischen Schulungen zur Informationssicherheit und zum Datenschutz teil.

Igor Dobrovolskyi unterliegt den gleichen Anforderungen wie unsere eigenen Mitarbeiter in Deutschland. phase6 kümmert sich sowohl um die Bereitstellung und Wartung der Hard- und Software als auch um die Weiterbildung. Hr. Dobrovolskyi arbeitet stets aus dem Home-Office, das den gleichen Anforderungen an den Arbeitsplatz unterliegt, wie dies in unseren deutschen Büros der Fall ist und über eine 2-fach redundante Internetverbindung als auch einen Stromgenerator verfügt. Wie oben bereits angemerkt, ist Hr. Dobrovolskyi in besonderem Maße für Datenschutz sensibilisiert, da er eine wichtige Rolle bei der Umsetzung unserer Anforderungen spielt und so automatisch an allen die IT betreffenden Prozessen teilnimmt.

Risiko der verarbeiteten Datenkategorien:
- Kontaktdaten (nur E-Mail, Vorname, Nachname - sofern angegeben)
- Lernfortschritt und ggfs. der Inhalt selbst angelegter Kärtchen

Kriegszustand in der Ukraine (zuletzt aktualisiert am 05.07.2023):

Trotz des Kriegszustandes in der Ukraine gibt es derzeit keine Änderungen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten. Die Gesetze sind in vollem Umfang in Kraft und wirksam.

Die Robustheit des ukrainischen IT-Sektors wurde bereits mehrfach auf die Probe gestellt, unter anderem durch den bewaffneten Konflikt und die Annexion der Krim in 2014 und zuletzt durch den aktuellen Kriegsausbruch in 2022. Der IT-Sektor wurde dabei in besonderem Maße geprüft, was zu besonderen Investitionen in die Informations- und Standortsicherheit führte. phase6 erhält regelmäßig und häufig Reports zur allgemeinen Gefahrensituation, Cyber Security, Sicherheit der Mitarbeiter, Mobilisierung und Leistungserbringung. Unsere ukrainischen Dienstleister haben während des Krieges bisher stets zuverlässig Ihre Leistung erbracht. Sicherheitsprobleme sind weder bekannt noch wurde bisher von entsprechenden Vorfällen berichtet.

Wahrscheinlichkeit von Zugriffsversuchen durch Behörden:
Die Wahrscheinlichkeit ist extrem gering, da:
- Ein solches Vorgehen nicht den Rechtsvorschriften und Gepflogenheiten der Ukraine entspricht
- Nur einzelne Datensätze verarbeitet werden
- Keine Daten verarbeitet werden, die für Behörden einen Wert darstellen (wie Verkehrs- und Verbindungsdaten, Adressdaten)
- Die Daten nur über (gesicherte) Verbindungen auf in Deutschland stehenden Servern der phase6 eingesehen werden.

Regelmäßige Überprüfung der Strategien und der Angemessenheit:
Aufgrund der fortlaufenden Entwicklung gibt es einen sehr intensiven und sehr regelmäßigen Austausch zum Thema Datensicherheit und Datensparsamkeit. Die Angemessenheit der Maßnahmen wird regelmäßig überprüft.

Verpflichtungen des Datenimporteurs:
Unsere Partner haben sich dazu verpflichtet, keine Weiterübermittlung personenbezogener Daten vorzunehmen.

## Sonstige optionale Auftragsverarbeiter

phase6 kann weitere Dienste Dritter verwenden, sofern der Nutzer dies möchte und in eine solche Nutzung aktiv und separat einwilligt. Dies wäre bspw. dann der Fall, wenn der Nutzer bei der Verarbeitung von Cookies einer weniger restriktiven Verarbeitung zustimmt oder durch Auswahl eines Zahlungsanbieters zur Zahlungsabwicklung.
Die Anpassung der Cookie-Verarbeitung kann per Voreinstellung gesperrt werden. Die gewünschte Verarbeitung wird bei Vertragsschluss entweder im Hauptvertrag (siehe “Strikter Modus”) oder in Anlage 3 geregelt. Darüber hinaus kann eine Einschränkung der Verarbeitung jederzeit nachträglich formlos per E-Mail an datenschutz@phase-6.de beantragt werden.

Aktuelle Informationen zu diesen Diensten Dritter sind stets in der Datenschutzerklärung von phase6 zu finden: https://www.phase-6.de/datenschutz_text.html

# Anhang 1 - Amplitude Inc.

Amplitude ist ein Dienst zur Produktnutzungsanalyse. Anhand der verarbeiteten Daten kann phase6 erkennen, welche Funktionen der App intensiv genutzt werden oder Probleme bereiten. phase6 kann beispielsweise über einen Zeitraum hinweg vergleichen, inwiefern App-Updates zum erstmaligen Nutzungserfolg und einer anschließenden dauerhaften Nutzung beitragen. Alle Daten werden regelmäßig und systematisch nur über das Datenzentrum von Amplitude in Deutschland verarbeitet.

## Vertragliche Regelungen (Auswahl):

[...]
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:
No sensitive data shall be submitted to the Services, unless the Agreement specifically permits the transfer of such data subject to any applicable restrictions and/or conditions, and even then, the extent of such transfer is determined and controlled by Customer in its sole discretion.
[...]
**Scope, Relationship of the Parties, and Data Use Limitations**
3. This DPA applies only to Personal Data that Customer submits to Amplitude as part of the Services, where such data is Customer Data and Services as defined in the Agreement.
4. Unless required by Applicable Law, Amplitude will Process the Personal Data only to: (i) perform the Services for Customer pursuant to the Agreement; (ii) comply with this DPA; and (iii) carry out Customer's reasonable written instructions that are consistent with the Agreement and this DPA. Without limiting the foregoing, (i) Amplitude shall not "sell" the Personal Data, as such term is defined in the CCPA; and (ii) Amplitude shall not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and Amplitude. Amplitude hereby certifies that it understands the restrictions and obligations set forth in this DPA and that it will comply with them.
5. If Amplitude receives a demand under Applicable Law to engage in Processing not permitted by the above, Amplitude shall attempt to redirect the demand to Customer and Customer agrees Amplitude may provide information as reasonably necessary for such redirect. If Amplitude cannot redirect the demand to Customer, Amplitude shall, to the extent legally permitted to do so, provide Customer reasonable notice of the demand as promptly as possible under the circumstances. This section does not diminish Amplitude's obligations under the Standard Contractual Clauses with respect to access by public authorities.
[...]
**Data Transfers**
27. If the customer selects the EU data center, Personal Data is systematically and regularly processed in the European Economic Area. In the event necessary to provide the Services, Customer authorizes Amplitude to make international transfers of the Personal Data only if (i) Applicable Law for such transfers is respected and (ii) the transfer is otherwise permitted by this DPA.
[...]

## Verfahren zu Wiedererkennung eines Nutzers:

**Aus unserer Datenschutzerklärung:**
"Die User ID, die Amplitude speichert, wird von phase6 übergeben und ermöglicht ein plattformübergreifendes Verständnis des Nutzerverhaltens. Bei der User ID handelt es sich um eine von phase6 pseudonymisierte ID, die bei Bedarf generiert und nicht in unserer eigenen Datenbank gespeichert wird. Eine Repersonalisierung dieser User ID ist theoretisch dann möglich, wenn der Algorithmus bekannt ist, voller Zugriff auf die Datenbank von phase6 besteht, erhebliche Ressourcen dafür eingesetzt werden und vollautomatischer maschinenlesbarer Zugriff auf die Amplitude Nutzerdaten bestehen.

Die Daten sind somit voneinander entkoppelt und gegen den Empfänger verschlüsselt.

## Katalog der verarbeiteten Daten

| Datenkategorien | Verarbeitung |
|---|---|
| **Adress- oder Kontaktdaten, Verbindungsdaten, Eindeutige Gerätekennungen:**<br>Apple IDFA (ID for Advertisers), GAID (Google Advertising ID), IP-Adressen | NEIN |
| **Genauer Standort:**<br>Longitude, Latitude | NEIN |
| **Erkennung wiederkehrender Nutzer anhand von IDs (Hashes):**<br>Amplitude ID (basiert unter iOS auf der IDFV)<br>UserID (von phase6 angereicherter Hash, sobald ein Nutzer registriert wurde) | JA |
| **App Ereignisse samt Eigenschaften mit Zeitstempel und Sitzungs-IDs:**<br>Nutzungsereignisse und Nutzungsaktivität und erhaltene Benachrichtigungen | JA |
| **Ungefährer Standort:**<br>Land, Bundesland, Stadt | JA |
| **Gerätedaten:**<br>Carrier, Gerätetyp, Gerätehersteller und Modell, Betriebssystem und Version, App Version, Amplitude Version, Plattform, Sprache | JA |
| **Informationen zum Nutzer:**<br>Rolle, Personalisierungseinstellungen wie Design oder Avatar, Benachrichtigungseinstellungen, in Familie, an Schule, Lernerinnerungsstatus, zahlender Nutzer, Schul-ID (Hash) | JA |
| **Herkunft bei Klick auf Werbe-Link:**<br>Werbenetzwerk und Informationen zur Kampagne oder Link-Verweise. Betrifft unter iOS Nutzer mit iOS Version 14.4 (Juni 2020) oder älter. Kann auf Android-Geräten vom Nutzer deaktiviert werden. | JA |

Die hier aufgelisteten Datenkategorien sind im Sinne der einfachen Verständlichkeit von phase6 zusammengefasst worden. Im Sinne der Datensparsamkeit wird der Umfang der erfassten Daten mindestens jährlich überprüft und ggfs. angepasst.

# Anhang 2 - Google LLC / Firebase Inc.

Firebase ist die Plattform von Google für die Entwicklung mobiler Anwendungen. Anhand der verarbeiteten Daten kann phase6 zusätzliche Funktionen anbieten, beispielsweise um dem Nutzer die Anmeldung zu erleichtern, auf Abstürze zu reagieren, Lernerinnerungen zu senden, den Werbeerfolg auszuwerten oder Konfigurationsanpassungen ohne Update zur Verfügung zu stellen. phase6 verwendet darüber hinaus den Google Tag Manager.
Der GTM ist nicht direkt eingebunden, sondern über sogenanntes “Server Side Tagging”. So agiert phase6 als Proxy oder Vermittler und schließt damit aus, dass IP-Adressen potentiell verarbeitet werden könnten.

| Service | End-user data | How data helps to provide the service |
|---|---|---|
| Firebase Cloud Messaging | Firebase Installation IDs | How it helps: Firebase Cloud Messaging uses Firebase installation IDs to determine which devices to deliver messages to.<br><br>Retention: Firebase retains Firebase installation IDs until the Firebase customer makes an API call to delete the ID. After the call, data is removed from live and backup systems within 180 days. |
| Firebase Crashlytics | Crashlytics Installation UUIDs<br>Crash traces<br>Breakpad minidump formatted data (NDK crashes only) | How it helps: Firebase Crashlytics uses crash stack traces to associate crashes with a project, send email alerts to project members and display them in the Firebase Console, and help Firebase customers debug crashes. It uses Crashlytics Installation UUIDs to measure the number of users impacted by a crash and minidump data to process NDK crashes. The minidump data is stored while the crash session is being processed and then discarded. Refer to Examples of stored device information for more detail on the types of user information gathered.<br><br>Retention: Firebase Crashlytics retains crash stack traces, extracted minidump data, and associated identifiers (including Crashlytics Installation UUIDs) for 90 days. |
| Firebase Remote Config | Firebase Installation IDs | How it helps: Remote Config uses Firebase installation IDs to select configuration values to return to end-user devices.<br><br>Retention: Firebase retains Firebase installation IDs until the Firebase customer makes an API call to delete the ID. After the call, data is removed from live and backup systems within 180 days. |
| Google Analytics for Firebase* | ~~Mobile ad IDs~~<br>IDFVs/~~Android IDs~~<br>Firebase installation IDs<br>Analytics App Instance IDs | How it helps: Google Analytics for Firebase uses the data to provide analytics and attribution information. The precise information collected can vary by the device and environment. For more information see Data collection.<br><br>Retention: Google Analytics for Firebase retains certain advertising identifier associated data (e.g., ~~Apple’s Identifier for Advertisers~~ and Identifier for Vendors, ~~Android’s Advertising ID~~) for 60 days, and retains aggregate reporting without automatic expiration. Retention of user-level data, including conversions, is fixed at up to 14 months. For all other event data, you may set the retention in your Google Analytics for Firebase settings to 2 months or 14 (**) months. |

* Die Dienste befinden sich im Review und die weitere Verwendung wird fortlaufend abgewogen.
** Von phase6 verwendete Einstellung