PRIVACY4KIDS
LERNMATERIAL
VERSION 1.0
APRIL 2022

Eine Kooperation zwischen:

dsb Republik Österreich Datenschutzbehörde

universität wien
Institut für Innovation und Digitalisierung im Recht

1. ALLGEMEINE INFORMATIONEN

Dieser Leitfaden unterstützt Lehrer:innen, das Thema „Datenschutz für Kinder und Jugendliche“ im Unterricht zu behandeln. Auf der Website unter www.privacy4kids.at befinden sich Lernvideos. Diese Videos wurden in Kooperation zwischen der Datenschutzbehörde und der Universität Wien u.a. konzipiert. Pro Thema gibt es zwei Videos, jeweils für die Alterszielgruppe 6-10 Jahre und 10-14 Jahre.

Zusammengefasst geht es in den Videos um den Schutz personenbezogener Daten, Rechte der betroffenen Personen, welche Gefahren für ihre Privatsphäre im Internet bestehen und wie sie sich vor Betrug im Netz und Manipulation in sozialen Medien schützen können:

Video 1: Social Media & Influencer
Video 2: Internet Betrug & Phishing
Video 3: Apps
Video 4: Preisgabe persönlicher Daten
Video 5: Big Brother is watching you
Video 6: Gaming
Video 7: Hass im Netz
Video 8: Rechte der betroffenen Person
Video 9: Cookies
Video 10: Digitaler Fußabdruck
Video 11: Social Media & Influencer

Es wird empfohlen, der Klasse im Unterricht jeweils ein bis zwei ausgewählte Videos über ein Gerät (etwa PC oder Tablet) vorzuspielen. Idealerweise wählen Sie die Videos zu einem Thema, welches Ihrer Meinung nach für die Klasse gerade aktuell ist.
Im Anschluss können Sie mit den Kindern diskutieren, worum es bei den Videos geht.
Es wird empfohlen, wie folgt vorzugehen:

1. **Die Klasse schaut sich gemeinsam ein bis zwei Videos an.**
2. **Es wird anschließend über den Inhalt der Videos diskutiert.**
   Die Diskussion kann sich um folgende Aspekte drehen:
   – Wer waren die Hauptpersonen?
   – Hatten die Hauptpersonen Angst und warum?
   – Hatte die Geschichte ein gutes Ende?
   – Welche Botschaft soll das Video vermitteln?
3. **Abschließend stellen Sie der Klasse Übungsfragen zu den vorgespielten Videos, welche von der Klasse schriftlich oder mündlich beantwortet werden sollen. In weiterer Folge werden einige Übungsfragen als Beispiel zur Verfügung gestellt.**
4. **Der ungefähre Zeitrahmen sollte wie folgt aussehen:**
   – jedes Video ist ungefähr 2 bis 3 Minuten lang
   – Diskussion pro Video: 20 bis 30 Minuten
   – Übungsfragen: 10 bis 15 Minuten

Bitte achten Sie darauf, dass Sie das Video für die passende Alterszielgruppe (6-10 Jahre und 10-14 Jahre) auswählen.

2. ÜBUNGSFRAGEN FÜR ANSCHLIESSENDE DISKUSSION

Nachfolgend werden pro Video einige Übungsfragen als Beispiel bereitgestellt.
Diese Übungsfrage können Sie Ihrer Klasse stellen, um eine Diskussion anzuregen.
Bei jeder Übungsfrage finden Sie auch die passende Antwort zur Auflösung der Frage.
Grundsätzlich können die Übungsfragen beiden Alterszielgruppen gestellt werden.
Bei manchen Videos werden aber auch altersspezifische Übungsfragen bereitgestellt.

VIDEO 1 / SOCIAL MEDIA & INFLUENCER

VIDEO 1 / 1. ÜBUNGSFRAGE:

Ist es zulässig, Fotos von anderen Personen im Internet zu veröffentlichen, ohne dass diese Personen darüber Bescheid wissen?

ANTWORT FÜR LEHRPERSONAL:

Grundsätzlich ist es nicht zulässig. Es gibt Gesetze, die die Privatsphäre von Personen schützen. Eine Ausnahme kann bestehen, wenn es sich um bekannte Personen handelt, wie zum Beispiel Politiker oder Popstars. Zum Beispiel schützt die Datenschutz-Grundverordnung (DSGVO) das Grundrecht auf Datenschutz von Personen.

VIDEO 1 / 2. ÜBUNGSFRAGE:

Was wird unter Privatsphäre verstanden?

ANTWORT FÜR LEHRPERSONAL:

Dies stellt die Grenze der eigenen Würde, Identität und des Rechts dar, in die grundsätzlich nicht eingegriffen werden darf (siehe Blasenbeispiel im Video). Zum Beispiel geht es fremde Personen nichts an, mit welchen Freunden du dich triffst oder welche Websites du im Internet besuchst.

VIDEO 1 / 3. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 6-10 JAHRE):

Welche Möglichkeiten hat Geist Hugo, sodass er seine Daten schützt?

ANTWORT FÜR LEHRPERSONAL:

Er kann die Löschung seiner personenbezogenen Daten (wie Name, Vorname, Adresse, etc.) beantragen. Er kann die Lehrer:innen und Eltern um Hilfe bitten.

VIDEO 2 / INTERNET BETRUG & PHISHING

VIDEO 2 / 1. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 6-10 JAHRE):

Wofür stehen der Hai und die Fische hier im Video?

ANTWORT FÜR LEHRPERSONAL:

Der Hai ist ein Betrüger:innen und die Fische sind Daten bzw. Informationen von anderen Personen.

VIDEO 2 / 2. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 6-10 JAHRE):

Was passiert mit den Fischen (Daten), wenn diese in den Fluss gelangen?

ANTWORT FÜR LEHRPERSONAL:

Diese können in der Regel nicht mehr zurückgeholt werden. Der Betrüger:innen kann die Daten dann verwenden.

VIDEO 2 / 3. ÜBUNGSFRAGE:

Was wird unter „Phishing“ verstanden?

ANTWORT FÜR LEHRPERSONAL:

Im Internet gibt sich jemand als eine andere Person aus und versucht Daten von anderen Personen zu stehlen. Siehe auch: www.datenschutz-praxis.de/datenschutzbeauftragte/phishing-simulationen-darauf-muessen-sie-achten/

VIDEO 2 / 4. ÜBUNGSFRAGE:

Wie kannst Du Dich vor den Betrüger:innen im Internet schützen?

ANTWORT FÜR LEHRPERSONAL:

Gib dein Passwort niemals einer anderen Person. Dein Passwort sollte nicht „1234“ oder sogar dein Geburtstag sein, da dies leicht zu erraten ist.

Teile deine persönlichen Informationen wie deine Wohnadresse auch mit keinen fremden Personen.

VIDEO 3 / APPS

VIDEO 3 / 1. ÜBUNGSFRAGE:

Was muss vor der Verwendung einer App gemacht werden, dass deine Standortdaten (also wo du dich aufhältst) nicht gesammelt werden können?

ANTWORT FÜR LEHRPERSONAL:

Nach dem Einloggen in die App kann festgelegt werden, welche Daten preisgegeben werden. Bei vielen Apps kann die Standorterfassung ausgeschaltet werden.

VIDEO 3 / 2. ÜBUNGSFRAGE:

Wie können unangenehme Begegnungen wie im Video vermieden werden?

ANTWORT FÜR LEHRPERSONAL:

So wenige personenbezogene Daten wie möglich veröffentlichen. Adressdaten und Standorte sollten nicht veröffentlicht werden.

VIDEO 3 / 3. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 10-14 JAHRE):

Welche Grundeinstellungen könnt Ihr am Smartphone vornehmen, damit eure Smartphone-Daten nicht gesammelt und verkauft werden?

ANTWORT FÜR LEHRPERSONAL:

Bei einem Smartphone gibt es normalerweise bei den Einstellungen den Punkt „Datenschutz“ oder „Privacy“. Dort kann man datenschutzfreundliche Einstellungen vornehmen, wie zum Beispiel „Kontakte nicht teilen“ oder „personalisierte Werbung unerwünscht“. Darüber hinaus kann man dort Ortungsdienste deaktivieren.

HINWEIS FÜR LEHRPERSONAL:
Sie können Ihre Klasse auch ersuchen, am eigenen Smartphone bei den Einstellungen den Punkt „Datenschutz“ oder „Privacy“ zu suchen. Diskutieren Sie im Anschluss mit der Klasse, welche Einstellungsmöglichkeiten dort vorhanden sind.

VIDEO 4 / PREISGABE PERSÖNLICHER DATEN

VIDEO 4 / 1. ÜBUNGSFRAGE:

Warum gibt es „Fake“ Gewinnspiele?

ANTWORT FÜR LEHRPERSONAL:

Es wird von Betrügern vorgetäuscht, dass ein Gewinnspiel stattfindet. Damit wollen Betrüger unerlaubterweise Daten sammeln, wie zum Beispiel Name, Adresse oder Bankdaten.

VIDEO 4 / 2. ÜBUNGSFRAGE:

Was macht man, wenn fremde Personen im Internet aufdringlich sind und fragen, wo man wohnt?

ANTWORT FÜR LEHRPERSONAL:

Der fremden Person auf keinen Fall antworten und sich Hilfe bei den Eltern oder Lehrer:innen holen. Viele soziale Netzwerke wie Facebook oder TikTok bieten auch die Möglichkeit, dass man fremde Personen blockiert (Blockierfunktion).

VIDEO 4 / 3. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 10-14 JAHRE):

Bedeutet ein Symbol in Form eines Schlosses im Internetseitennamen (also der „Adresszeile“), dass es sich um eine sichere Internetseite handelt?

ANTWORT FÜR LEHRPERSONAL:

Nein. Ein solches „Schloss Symbol“ bedeutet einfach gesagt nur, dass die Verbindung zur Internetseite „sicher“ (verschlüsselt) ist. Leider verwenden aber immer mehr Betrüger (zum Beispiel Phishing-Seiten) auch ein solches „Schloss Symbol“. Man muss daher trotzdem sehr achtsam sein, welche Daten man auf einer Internetseite offenlegt.

VIDEO 5: BIG BROTHER IS WATCHING YOU

VIDEO 5 / 1. ÜBUNGSFRAGE:

Warum sollte sich Lars die App nicht herunterladen?

ANTWORT FÜR LEHRPERSONAL:

Weil er sonst in das „Datenklauland" kommt. Hier werden sämtliche personenbezogene Daten über Lars und andere Kinder gesammelt. So wird zum Beispiel berechnet, welche Vorlieben Lars hat. Damit können die Unternehmen Lars personalisierte Werbung schicken.

Bei manchen Programmen kann man das Sammeln von Daten und personalisierte Werbung verhindern, indem dies ausgeschaltet wird.

VIDEO 5 / 2. ÜBUNGSFRAGE:

Welche Programme oder Apps fallen euch ein, bei denen Daten gesammelt werden?

ANTWORT FÜR LEHRPERSONAL:

Dies sind beispielsweise Fitnessapps, bei denen Gesundheitsdaten, wie etwa Körpergröße, Gewicht, etc. gesammelt werden.

VIDEO 6: GAMING

VIDEO 6 / 1. ÜBUNGSFRAGE:

Worauf sollte beim „Gaming" besonders geachtet werden, sodass der böse Datensammler „Darth Data Collector" nur sehr wenige Daten sammeln kann?

ANTWORT FÜR LEHRPERSONAL:

Personen sollten so wenige Daten wie möglich preisgeben.

VIDEO 6 / 2. ÜBUNGSFRAGE:

Was bedeutet „Social engineering" und wie kann man sich davor schützen?

ANTWORT FÜR LEHRPERSONAL:

Bei „Social engineering" werden Personen von Betrügern beeinflusst. Die Betrüger wollen dabei an gewisse Informationen von euch kommen und versuchen, ein bestimmtes Verhalten von euch zu provozieren. So könnten die Betrüger etwa eure Passwörter stehlen.

VIDEO 7: HASS IM NETZ

VIDEO 7 / 1. ÜBUNGSFRAGE:

Welche Folgen hat es, wenn man etwas böses über eine andere Person im Internet veröffentlicht?

ANTWORT FÜR LEHRPERSONAL:

Toni fühlt sich verletzt und ist traurig. Im Video hatte es die Konsequenz, dass Toni nicht mehr in die Schule gehen will. Die Person, welche Hasskommentare gegen Toni schreibt, muss damit rechnen, dass die Eltern, Lehrer:innen und auch die Polizei eingeschaltet werden.

VIDEO 7 / 2. ÜBUNGSFRAGE:

Was können Personen tun, welche mit „Hass im Netz" (zum Beispiel Hass-Kommentaren auf Instagram) konfrontiert sind?

ANTWORT FÜR LEHRPERSONAL:

Diese können sich an die Eltern, Geschwister oder an die Lehrer:innen wenden, sodass diese helfen können. In Folge können diese eine Meldung an die Plattform (wie Instagram) abgeben, sodass der Hasskommentar gelöscht wird.

Auch eine Meldung an die Polizei ist bei Hasskommentaren möglich.

VIDEO 8: RECHTE DER BETROFFENEN PERSON

VIDEO 8 / 1. ÜBUNGSFRAGE:

Was kann von der Datendiebin in Bezug auf die eigenen Daten verlangt werden?

ANTWORT FÜR LEHRPERSONAL:

Beispielsweise die Löschung der verarbeiteten personenbezogenen Daten.

VIDEO 8 / 2. ÜBUNGSFRAGE:

Wie kann ein Selfie „hochgeladen" werden, ohne dass zu viele Daten in das Internet gelangen?

ANTWORT FÜR LEHRPERSONAL:

Dazu kann man beispielsweise die Standorterfassung in den Einstellungen deaktivieren und das Profil bzw. den Beitrag auf „nicht öffentlich" einstellen. Damit kann ein Profil bzw. der Beitrag nur von Freunden gesehen werden, nicht jedoch auch von fremden Personen.

VIDEO 9: COOKIES

VIDEO 9 / 1. ÜBUNGSFRAGE:

Was versteht ihr unter „Cookies“?

ANTWORT FÜR LEHRPERSONAL:

Vereinfacht gesagt können Cookies dazu verwendet werden, um eure Vorlieben kennenzulernen. Cookies sind Textinformationen, die auf eurem Gerät (etwa Laptop) gespeichert werden. Wenn ihr beispielsweise im Internet surft, dann kann es sein, dass eure Vorlieben von Werbeunternehmen gespeichert werden und euch personalisierte Werbung angezeigt wird.

Wenn ihr zum Beispiel öfter im Internet nach Sportschuhen gesucht habt, kann es sein, dass euch dann oft Werbung für Sportschuhe angezeigt werden. Ihr könnt euch schützen, indem ihr regelmäßig die Browserdaten löscht. Darüber hinaus könnt ihr euch schützen, indem ihr auf „Cookies ablehnen“ (anstatt „Cookies akzeptieren“) klickt, wenn ihr eine solche Auswahl habt.

VIDEO 9 / 2. ÜBUNGSFRAGE (NUR FÜR ALTERSZIELGRUPPE 10-14 JAHRE):

Warum sagt man, dass „Cookie Banner“ manchmal irreführend gestaltet sind?

ANTWORT FÜR LEHRPERSONAL:

Es kann der Fall sein, dass beim Aufruf einer Internetseite beim „Cookie-Banner“ die Option „Alle Cookies akzeptieren“ gut sichtbar ist, während die Option „Cookies nicht akzeptieren“ nur schwer erkennbar ist. Dies liegt daran, dass Betreiber einer Internetseite ein Interesse daran haben, dass möglichst viele Personen Werbe-Cookies akzeptieren.

Dadurch können die Betreiber (vereinfacht gesagt) zielgerichtete Werbung auf ihrer Internetseite anzeigen. Das nennt man auch „nudging“ (was übersetzt „anstupsen“) bedeutet. Eine irreführende Gestaltung eines „Cookie Banner“ ist jedenfalls unzulässig.

VIDEO 10: DIGITALER FUSSABDRUCK

VIDEO 10 / 1. ÜBUNGSFRAGE:

Was kann unter einem „digitalen Fußabdruck“ verstanden werden?

ANTWORT FÜR LEHRPERSONAL:

Vereinfacht gesagt merkt sich das Internet, welche Websites man besucht hat. Im Internet können viele Informationen gespeichert werden, wie auch das Surfverhalten.

So kann gespeichert werden, nach welchen Dingen man in der Vergangenheit im Internet gesucht hat. Hat man zum Beispiel oft nach Sportschuhen im Internet gesucht, so ist es wahrscheinlich, dass in Folge im Internet sehr oft Werbung für Sportschuhe angezeigt wird. Dies nennt man auch „personalisierte Werbung“.

VIDEO 10 / 2. ÜBUNGSFRAGE:

Warum ist der „digitale Fußabdruck“ gefährlich?

ANTWORT FÜR LEHRPERSONAL:

Euer Leben wird sehr stark vom Internet beeinflusst. Es ist gefährlich, weil bestimmte Unternehmen viele Daten über euer Nutzerverhalten haben und wissen, was ihr mögt und nicht mögt.

VIDEO 10 / 3. ÜBUNGSFRAGE (ERST AB 12 JAHREN EMPFOHLEN):

Warum sollte man keine Nacktbilder („nudes“) im Internet verschicken oder veröffentlichen?

Antwort für Lehrpersonal:

Das Internet vergisst nicht. Es kann sein, dass eure Fotos oder Videos irgendwann in die falschen Hände gelangen und von Personen mit bösen Absichten verbreitet werden. Es wird dann sehr schwierig oder unmöglich, die Fotos oder Videos löschen zu lassen. In manchen Fällen kann es sogar sein, dass euch Personen erpressen wollen („Gib mir Geld oder ich veröffentliche deine Fotos“). Wenn ihr doch in eine solche Situation kommt, sucht euch Hilfe bei einer Person eures Vertrauens und geht gemeinsam zur Polizei.

VIDEO 11: SOCIAL MEDIA & INFLUENCER

VIDEO 11 / 1. ÜBUNGSFRAGE:

Warum soll Alex der unbekannten Person keine Informationen geben?

ANTWORT FÜR LEHRPERSONAL:

Die unbekannte Person kann Alex verfolgen, überwachen und bedrängen.

VIDEO 11 / 2. ÜBUNGSFRAGE:

Was kann Alex tun, damit Sie nicht in eine solche schlimme Situation kommt?

ANTWORT FÜR LEHRPERSONAL:

Damit es gar nicht erst zu einer solchen Situation kommt, könnte Alex ihr Social Media Profil in den App Einstellungen auf „privat" einstellen. Damit können fremde Personen wie Magisch 34 ihre Beiträge erst gar nicht sehen.

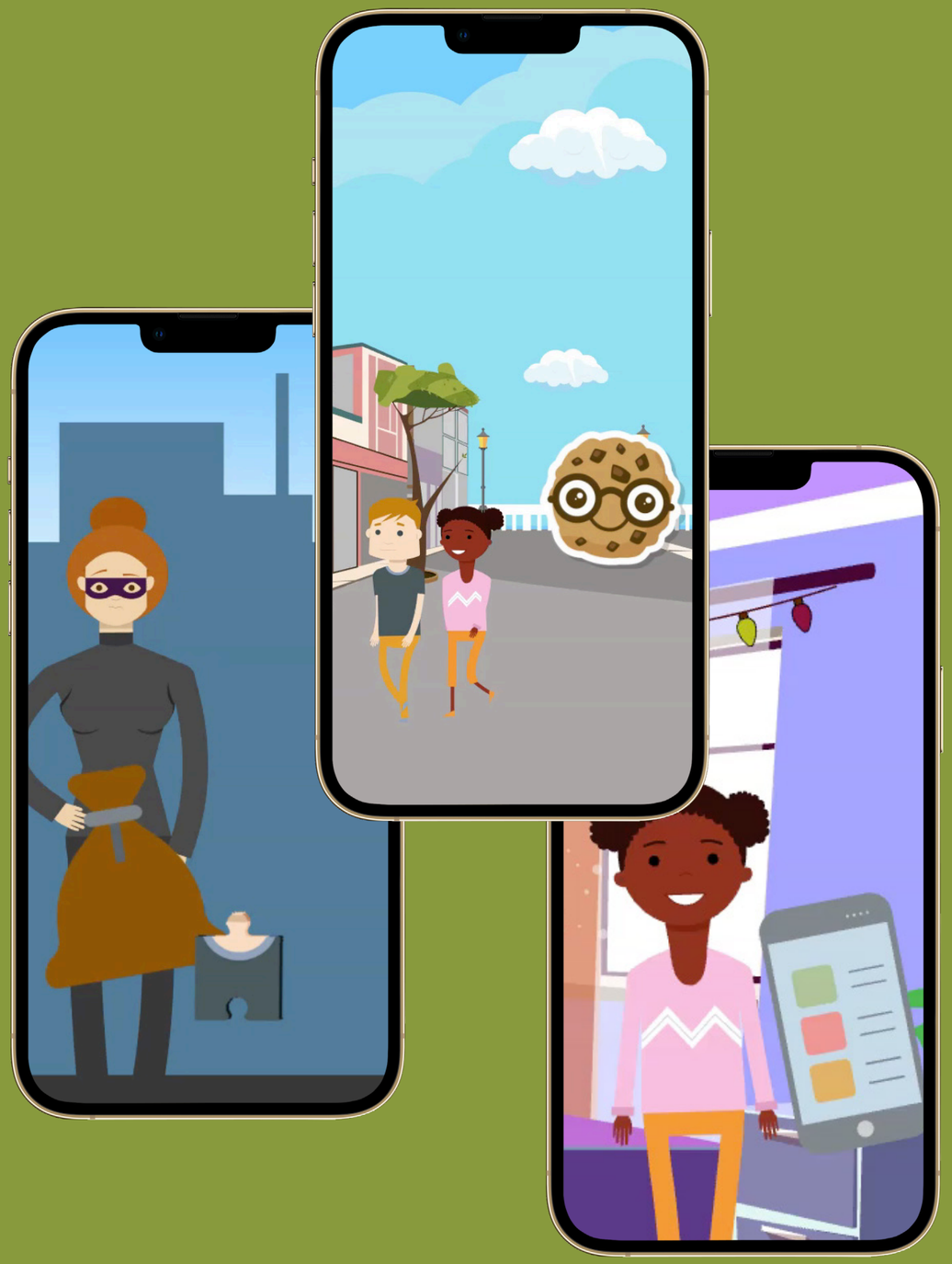
VIDEO 11 / 3. ÜBUNGSFRAGE:

Was kann man tun, wenn eine fremde Person im Internet wissen will, wo man wohnt?

ANTWORT FÜR LEHRPERSONAL:

Wenn dich eine fremde Person im Internet anschreibt und du das nicht willst, sage das der fremden Person. Gib deine Wohnadresse nicht bekannt, auch wenn dir die fremde Person freundlich vorkommt.

Wenn dich die fremde Person weiterhin anschreibt, blockiere die fremde Person am besten. Das kannst du in den Einstellungen des sozialen Netzwerks oder des Chat-programms tun. Darüber hinaus gibt es bei den meisten sozialen Medien die Mög-lichkeit, diese Person auch zu melden („Meldefunktion"). Wenn du in einer solchen Situation bist, hole dir auch Hilfe von deinen Eltern oder Lehrer:innen.



PRIVACY4KIDS

IMPRESSUM
Diese Unterlagen wurden gemeinsam von der Datenschutzbehörde Österreich und der Universität Wien (Institut für Innovation und Digitalisierung im Recht) erstellt.

ÖSTERREICHISCHE DATENSCHUTZBEHÖRDE
Barichgasse 40-42
1030 Wien
T: +43152152-0
E: dsb@dsb.gv.at

INSTITUT FÜR INNOVATION UND DIGITALISIERUNG IM RECHT
Schenkenstraße 4/2.Stock
1010 Wien
T: +43-1-4277-34201
E: ID-organisation@univie.ac.at

Für weitere Informationen zu privacy4kids besuchen Sie die Website
www.privacy4kids.at

Dieses Projekt wurde vom Programm
„Rechte, Gleichstellung und Unionsbürgerschaft“
der Europäischen Union (2014-2020) finanziert.