Privacy Policy der ESBZ

| :--- | :--- | | Version | 0.8 / 27.02.2019 | | Autoren | Mira, Anton, Bernhild, Steini, derMicha | | Kontakt | gruppe-digital@esbz.org |

Ziel

Die ESBZ definiert in ihrem digitalen Leitfaden ihre Position zum Umgang mit digitalen Medien und Netzen. Aus diesem Selbstverständnis leiten sich konkrete Vorgaben für den Einsatz digitaler Technologien an der Schule und im Unterricht ab. Diese Privacy Policy hat das Ziel über die DSGVO hinausgehen Vorgaben zum Schutz der Privatsphäre der Schulgemeinschaft zu machen.

Die nachstehenden Vorgaben sind verbindlich. Ausnahmen müssen vom Ausschuss Digitale Agenda geprüft und genehmigt werden.

1. Grundlagen

1. Unter sensiblen Daten verstehen wir personenbezogene Daten wie z.B.: Name, Adressen, Bewertungen/Beurteilungen, Vorlieben, Abneigungen, Interessen, Beziehungen, zeitliche und/oder räumliche Nutzungsdaten, Video/Bild/Ton-Aufnahmen von Menschen (Persönlichkeitsrechte sind einzuhalten).
2. Sensible Daten sollen ausschließlich von qualifizierten und autorisierten Personen bearbeitet werden können. Weiterhin müssen diese Personen die Privacy Policy des ESBZ durch eine Unterschrift explizit akzeptieren.
3. Als verschlüsselt gelten Daten, wenn sie mit Stand heutiger Technik als verlässlich eingestuften Algorithmen[1] (AES, RSA, ECC) verschlüsselt wurden und wenn mindestens die vom BSI empfohlene Schlüssellängen[2] verwendet wurden. Die eingesetzte Software muss unseren Software Regeln [3] entsprechen.
4. Für alles, nicht explizit in der Privacy Policy geregelte, gilt die DSGVO[4].
5. Besonders sensible Daten wie Video/Bild/Ton-Aufnahmen von Mitgliedern der Schulgemeinschaft dürfen nur innerhalb der Schulgemeinschaft verwendet und gespeichert werden.
6. Persönliche Daten der Schüler*innen, der Eltern sowie der Mitarbeiter*innen sind in besonderem Maß zu schützen.

[1] BSI Infos zu Algorithmen und Schlüssellängen
[2] BSI Infos zu Algorithmen und Schlüssellängen
[3] siehe 1.8 Von der Schulgemeinschaft eingesetzte Software
[4] Infos zum Datenschutz von der EU: https://ec.europa.eu/info/privacy-policy_de

7. Lokale Datenverarbeitung und -speicherung:
   (a) Sensible Daten dürfen nur lokal (in der Schule) und verschlüsselt[5] gespeichert (z.B. 4) werden.
   (b) Die Systeme und Services müssen durch Passworte[6] geschützt sein, die dem Passwort-Standard[7] der ESBZ entsprechen.
   (c) Die Daten verarbeitenden Systeme müssen dem Stand der Technik entsprechen und permanent aktuell gehalten werden. Insbesondere sind Sicherheits-Updates unmittelbar nach Erscheinen einzuspielen.
8. Von der Schulgemeinschaft eingesetzte Software muss diesen Kriterien genügen:
   (a) Der Source Code muss einsehbar sein, und/oder
   (b) Die Software ist durch ein unabhängiges Audit gegangen, bei dem der Source Code eingehend geprüft wurde und das Audit wird regelmäßig wiederholt. und/oder
   (c) Ein unabhängiges Gremium muss diese geprüft und frei gegeben haben (z.B. Ausschuss Digitale Agenda)

2. Datenübertragung

1. Sensible Daten dürfen nur verschlüsselt übertragen werden.
2. Ein Ausspähen der Daten muss nach Stand der Technik verhindert werden.

3. Cloud Services:

1. Sensible Daten dürfen nur verschlüsselt auf Cloud-Services gespeichert werden.
2. Daten dürfen nur bei solchen Cloud Diensten verarbeitet werden, bei denen die Erfüllung des Datenschutzes überprüft werden kann. D.h.:
   (a) Die Services werden selbst durch qualifiziertes und autorisiertes Personal betrieben, oder
   (b) Es müssen unsere Software Regeln (1.8) eingehalten werden
3. Die tatsächlich genutzten Systeme müssen sich physikalisch in der Europäischen Union befinden und dürfen sensible Daten nicht an Systeme außerhalb des Geltungsbereichs der DSGVO2 versenden.
4. Der Gerichtsstand der Cloud Service Anbieter muss sich in der EU befinden.

[5] Veracrypt, Sicherheitsüberprüfung von Veracrypt
[6] Gute Passwörter
[7] siehe 6. Passwort Standard

4. Datensparsamkeit:

1. Es dürfen nur solche Daten erhoben werden, die zwingend und aus dokumentiertem Grund erforderlich sind. Ein unabhängiges Gremium prüft und bestätigt die Notwendigkeit. (Beispiel: es ist nicht notwendig bei der Anmeldung zu Bettermarks bzw. Rosetta Stone etc. Klarnamen zu verwenden).
2. Bei einer Änderung des Status (Schulwechsel, Abschluss, etc.) müssen alle nicht mehr erforderlichen Daten innerhalb der gesetzlich vorgeschriebenen Fristen gelöscht werden.
3. Wir achten immer darauf, keine Entscheidung über sensible Daten von Dritten zu treffen (Upload von Adressbüchern, veröffentlichen von Bildern, ...).
4. Die Schulgemeinschaft verpflichtet sich Adblocker[8] zu verwenden.

5. Transparenz:

1. Die Schule führt ein Verzeichnis über die Speicherung und Verwendung aller personenbezogenen Informationen und des Verwendungszwecks. Das Verzeichnis ist den Mitgliedern der Schulgemeinschaft zugänglich zu machen.
2. Es wird die generelle Regel[9] der Schule zum Umgang mit Video/Bild/Ton-Aufnahmen eingehalten, Ausnahmen sind nur mit expliziter Zustimmung der Betroffenen (und deren juristische Vertretung) zulässig.

6. Passwort Standard

1. Dieser Standard ist von der Schulgemeinschaft anzustreben und verpflichtend, sobald sensible Daten Dritter betroffen sind.
2. Passwörter sind als sicher zu betrachten, wenn sie folgende Kriterien erfüllen[10]:
   (a) Passwörter dürfen nur einmalig verwendet werden.
   (b) Passwörter sind mindestens 13 Zeichen
   (c) Sie enthalten Zahlen, Ziffern sowie Groß- und Kleinschreibung und mindestens ein Sonderzeichen.
   (d) Die Zeichenfolge darf keinen sinnvollen Text ergeben, darf nicht leicht zu erraten und sollte möglichst zufällig sein

[8] Adblocker Ghostery, oder aber EFF
[9] siehe 1.5 Persönliche Daten
[10] Gute Passwörter

3. Die Nutzung von Passwortsafes ist anzustreben
4. Wenn möglich sollte (insbesondere für besonders kritische System) eine 2 Faktor Authentifizierung[11] verwendet werden.
5. Zugänge (Cloud) sind prinzipiell personalisiert.

7. Lokale Netzwerk- / Serverinfrastruktur

1. Die internen Netze zum Zwecke des Unterrichts müssen physikalisch oder logisch (vlan) von dem Verwaltungsnetz getrennt sein.
2. Das Verwaltungsnetz ist gegen unbefugte Nutzung besonders zu schützen. Insbesondere ist der Zugang auf wohldefinierte Computer zu beschränken.
3. Alle sensiblen Informationen wie z.B. Verbindungszeiten, Verweildauer, verwendete Hardware etc. dürfen ausschließlich lokal oder auf Services nach Maßgabe der o.g. Richtlinien verarbeitet werden und nur dann erhoben werden, wenn dies aus nachvollziehbarem Grund unbedingt erforderlich ist [12].
4. Der Zugang zu den Geräten der Netzwerkinfrastruktur ist verschlossen zu halten.
5. So weit wie rechtlich und technisch möglich vermeiden wir das Erzeugen von Protokolldateien [13].

8. Suchmaschinen und Socialmedia

1. Im Schulalltag dürfen ausschließlich Suchmaschinen verwendet werden, die eine anonyme Suche ermöglichen, Aussnahmen müssen im Ausschuss Digitale Agenda bewilligt werden
2. Es dürfen nur den Cloud Services [14] entsprechende Socialmedia Services verwendet werden, idealer Weise sind selbst betriebene dezentrale Lösungen zu verwenden

9. Vorgaben zur Nutzung des Internets im Unterricht

1. Lehrerinnen und Lehrer dürfen den Schülerinnen und Schülern ausschließlich Cloud-Services empfehlen, die den Maßgaben der Cloud Services

[11] 2FA Lösungen von Yubico oder Nitrokey
[12] siehe Datensparsamkeit
[13] siehe Datensparsamkeit
[14] siehe Cloudservices

[15] entsprechen. Ausnahmen sind durch den "Ausschuss Digitale Agenda" zu genehmigen.

2. Pädagog*innen sollen Vorbildfunktion übernehmen
3. Open Source Software ist wegen besserer Transparenz zu bevorzugen
4. Datensparsamkeit soll immer angestrebt werden, welche Daten müssen wirklich erhoben werden?
5. Vermitteln des Leitfaden und der Privacy Policy an die Schülerschaft und Pädagog*innen
   (a) es sollen Bausteine entstehen
   (b) Recht am eigenen Bild hat hohen Wert und muss im Zweifel immer berücksichtigt werden.

Relevante Links

1. ESBZ Wiki
2. digitalcourage
3. EFF
4. Cryptoparty

Erläuterungen zur privacy policy

zu 1.1: Meine Daten gehören mir

Personenbezogene Daten sind sensibel, da sich mit ihrer Hilfe Menschen eindeutig identifizieren lassen. Konzerne und Staaten sammeln im grossen Stil personenbezogene Daten und können schon anhand minimaler Anhaltspunkte Rückschlüsse auf die Identität der jeweiligen Person ziehen und diese eindeutig identifizieren.

zu 1.2: Ich kann meine Privatsphäre nicht schützen, wenn andere meine Privatsphäre mit Füßen treten

Der Umgang mit sensiblen Daten erfordert Problembewusstsein und verantwortungsvolles Handeln. Oft sind es nur Kleinigkeiten, Unwissen oder Missverständnisse und manchmal auch Arglosigkeit oder die hohe Arbeitsbelastung, die zu erheblicher Verletzung der Privatsphäre Dritter führt. Menschen, die mit sensiblen Daten hantieren, müssen darin geschult sein und zyklisch fortgebildet werden. Die Brisanz ist vergleichbar mit dem Hantieren mit Schadstoffen, Medikamente oder gefährlichen Gütern, da die Folgen ähnlich schwerwiegend sein können. Es

[15] siehe Cloudservices

kann nur verantwortungsvoll handeln, wer sich über die Konsequenzen im Klaren ist.

zu 1.3: Vertraue nicht der Werbung, nur überprüfbare Verschlüsselung ist gute Verschlüsselung

Viele kommerzielle Produkte verwenden schwache oder fehlerbehaftete Algorithmen und Verfahren oder die verwendeten Verfahren werden verschwiegen und lassen sich gar nicht einschätzen oder Überprüfen. Ob das dem Druck der "time to market", dem Unvermögen preiswerter und schlecht ausgebildeter Softwareentwickler oder dem Bedürfnis von Firmen und/oder Organisationen nach "Hintertüren" zum Ausspähen der Daten geschuldet ist, sei dahingestellt. Die Marketingversprechen werden oft genug nicht eingehalten, Grund misstrauisch zu sein. Gerade die Daten junger Menschen müssen mit kryptographischen Algorithmen geschützt werden, die auch noch sehr lange in die Zukunft hinein gegen Angriffe sicher sind. Denn auch verschlüsselte Daten werden langfristig gespeichert, in der Hoffnung, sie später mit schnelleren Computern und neuen Verfahren doch noch entschlüsseln zu können.

zu 1.4.: Die DSGVO ist geltendes Recht, das alle betrifft und schützen soll, aber die meisten Menschen kennen sie nicht

Die meisten hier definierten Punkte geben ohnedies die DSGVO wider bzw. präzisieren deren mitunter etwas vagen und interpretationsfähigen Regeln. Aber natürlich kann und will das hier vorliegende Regelwerk die DSGVO nicht außer Kraft setzen, sondern lediglich an einigen Punkten ergänzen bzw. aus guten und nachvollziehbaren Gründen verbessern.

zu 1.5: Schon ein Bild oder ein Satz kann mein ganzes Leben ruinieren

Das “Recht am eigenen Bild” ist bereits in der Gesetzgebung speziell definiert. Da auch Tonaufnahmen heute nahezu gleichermaßen verwerten werden können, fügen wir diese dem “Recht am eigenen Bild” hinzu. Aus Tonaufnahmen lassen sich die Sprechenden eindeutig identifizieren und aus Tonfall und Sprechweise Rückschlüsse auf persönliche Umstände und die Gemütsverfassung ableiten.

zu 1.6: Wer jung ist, über den kann man länger Daten sammeln

Insbesondere die Schule hat eine besondere Verantwortung, da genau hier eine besondere Menge und Qualität an Informationen anfallen, was Vorlieben, Abneigungen, Fähigkeiten und Beziehungen angeht und die Schutzbefohlenen sehr jung sind, deren Daten also noch sehr lange von relevanter Bedeutung für ihr zukünftiges Leben sein werden.

zu 1.7: Wer mit Daten hantiert, muss Standards einhalten

“Es wird schon nix passieren” hat sich schon immer als falsch erwiesen.

zu 1.8: Das Problem ist nicht der Angriff auf die Privatsphäre, sondern die schlechte Software, die dem nicht standhält.

Nur überprüfbare Software kann sichere Software sein. Selbst z.B. Autos und medizinische Heilmethoden werden ständig auf ihre Sicherheit hin überprüft, die Software, mit der diese Daten verarbeitet werden aber nicht. Das ist gefährlich und dumm. Ingenieur*innen, Techniker*innen, Ärzt*innen und so fort müssen Prüfungen ablegen und ihre Qualifikation nachweisen, Software Entwickler*innen nicht. Es gibt in diesem Bereich keine Standards, die einzuhalten sind. Daher obliegt die Prüfung der Software Qulität (noch) den Nutzer*innen und Anwender*innen.

zu 2: Das Internet ist die Wildnis

Niemand würde seine intimen Geheimnisse per Postkarte und seine Firmengeheimnisse an seine Wettbewerber verschicken. Im Internet passiert das aber ständig.

An jeder Weggabelung sitzen Söldner*innen mit dem Auftrag die Daten zu stehlen. Informationen sind Macht und Geld.

zu 3: Wo Daten sind kommen Daten weg

Die Presse ist voll von Meldungen, dass Unternehmen, Organisationen und Dienste den Verlust ihres kompletten Datenbestandes zu beklagen haben. Besser, wenn diese dann verschlüsselt waren.

zu 4. Der beste Schutz vor Datenverlust ist, Daten gar nicht erst zu sammeln

Das ist wie: “Die beste Methode mit dem Rauchen aufzuhören ist, gar nicht erst anzufangen”.

Daten, die nicht existieren, kommen nicht weg und die kann man nicht missbrauchen.

Völlig sorgenlos sind Menschen bereit, Firmen und Staaten ihre intimsten Geheimnisse mitzuteilen, die sie nicht mal mit ihren besten Freunden oder Freundinnen teilen würden.

Arglos treffen Menschen die Entscheidung für andere, deren privaten Daten z.B. in Form des eigenen Adressbuches auf die Server von Unternehmen mit Standorten in korrupten Staaten zu übertragen. In jedem einzelnen Fall ist es sinnvoll, zu überlegen, welche Daten zur Nutzung eines Dienstes zwingend erforderlich sind und ob es zum Nutzen des Dienstes wichtig ist, die Wahrheit zu sagen. Pseudonyme sind ein geeignetes Mittel um Privatsphäre zu schützen.

zu 5: Die Identität eines Menschen ist wie ein Kunstwerk aus Kristallglas.

Den Umgang mit sensiblen Daten kann man sich vorstellen wie das Ausleihen von etwas sehr Wertvollem und Zerbrechlichem. Es ist selbstverständlich dass man vor dem Ausleihen nachfragt, Bescheid sagt, was man damit tun will, sorgsam damit umgeht und es unbeschädigt zurück gibt.

zu 6: Was hilft das beste Schloss, wenn der Schlüssel steckt?

Passworte sind der Schlüssel zu einem Schatz. Je wertvoller der Schatz, um so sicherer sollte das Schloss sein.

zu 7: Eine Kette ist nur so stark wie das schwächste Glied

Die beste Zugangs-Sicherung hilft nichts, wenn sich ein Angreifer einfach in eine Netzwerkdose einstöpseln kann und *zack* auf alle Daten zugreifen kann.

zu 8: Es ist ein wichtiger Teil meiner Identität, wofür ich mich interessiere und wonach ich suche.

Suchmaschinen sammeln Daten über die Privatsphäre der Menschen. Mit jeder weiteren Suchanfrage komplettiert sich das Bild von Interessen, Vorlieben oder Obsessionen.

Das lässt sich vermeiden.

zu 9: Die Fähigkeit im Umgang mit Daten ist eine wichtige Voraussetzung für ein selbstbestimmtes Leben

Leider kann man von niemandem englisch lernen, der oder die selbst kein englisch kann. Kinder und Erwachsene lernen hier gemeinsam und voneinander. Die schockierende Brisanz des Kontrollverlustes über die eigenen Daten wird erst mit der Kenntnis über die Konsequenzen klar. Ähnlich wie beim Klimawandel und Massenaussterben werden die fatalen Folgen erst später sichtbar. Dann ist es aber zu spät und nicht mehr zu heilen.