CODE BLOCKS

Intern Document

In dit document vindt u:

- Een overzicht van alle persoonsgegevens die Codeblocks verwerkt en bewaart.
- De procedure bij datalekken en beveiligingsincidenten.
- Onze bewaartermijnen en afspraken met vrijwilligers.
- De externe partijen waarmee wij gegevens delen (zoals Firebase/Google).

Doel: dit document helpt Codeblocks om AVG-proof te werken en veilig met data om te gaan.

1. Verwerkingsregister

1.1 Accountgegevens (paneel)

- Welke gegevens: naam, e-mailadres, wachtwoord (hash, nooit in leesbare vorm), toegewezen rol/rechten in het systeem.
- Doel: het beheren van toegang tot het personeels- en lesportaal, zodat alleen bevoegde gebruikers bij modules en instellingen kunnen.
- Grondslag: toestemming van de vrijwilliger en/of uitvoering van de vrijwilligersovereenkomst.
- Opslaglocatie: Firebase Authentication (servers in de EU/VS).
- Toegang: uitsluitend voor het beheer.
- Beveiligingsmaatregelen:
  - Wachtwoorden worden nooit in platte tekst opgeslagen, alleen als hash.
  - Accounts zijn beschermd met rolgebaseerde toegang.
  - 2FA wordt verplicht voor beheerders.
- Bewaartermijn: zolang een account actief is. Bij beëindiging wordt het account gedeactiveerd en na maximaal 12 maanden volledig verwijderd.

1.2 Vrijwilligersgegevens

- Welke gegevens: naam, leeftijd, e-mailadres, Discord-naam, motivatie en – indien jonger dan 16 jaar – toestemming van ouder/verzorger.
- Doel: het verwerken van sollicitaties, beheren van vrijwilligers en onderhouden van communicatie binnen Codeblocks.
- Grondslag: toestemming van de vrijwilliger en, bij minderjarigen onder de 16 jaar, toestemming van de ouder/verzorger.
- Opslaglocatie: Firestore database (EU/VS) en Google Drive (voor documenten zoals de vrijwilligersovereenkomst).
- Toegang: uitsluitend voor het beheer en HR.
- Beveiligingsmaatregelen:
  - Gegevens worden opgeslagen binnen beveiligde omgevingen met rolgebaseerde toegang.
  - Alleen noodzakelijke gegevens worden verzameld.
  - Gevoelige documenten (zoals toestemmingsverklaringen) worden beperkt toegankelijk gemaakt.
- Bewaartermijn:
  - Bij afwijzing sollicitatie → maximaal 12 maanden bewaard, daarna verwijderd.
  - Bij actieve vrijwilligers → zolang de vrijwilliger betrokken is + maximaal 12 maanden na beëindiging.

1.4 Leerlinginteracties

- Welke gegevens: gekozen nickname (door de leerling zelf), sessiecode, antwoorden op vragen en behaalde resultaten.
- Doel: het uitvoeren van lessen en het geven van terugkoppeling aan docenten over voortgang en resultaten.
- Grondslag: uitvoering van een onderwijsactiviteit (les of demo) in samenwerking met een school.
- Opslaglocatie: Firestore database (EU/VS), binnen afgeschermde collecties per sessie.
- Toegang: docenten die de sessie uitvoeren en het beheer.
- Beveiligingsmaatregelen:
  - Leerlingen hoeven geen persoonlijk account aan te maken; alleen een nickname wordt gebruikt.
  - Gegevens zijn niet herleidbaar naar een specifieke leerling zonder aanvullende informatie van de school.
  - Resultaten zijn uitsluitend zichtbaar voor de docent van de sessie en het beheer.
  - Voor vragen of inzageverzoeken kunnen scholen en ouders contact opnemen via support: koen@codeblocks.nl.
- Bewaartermijn:
  - Leerlingresultaten worden maximaal 6–12 maanden bewaard.
  - Na deze termijn worden de gegevens geanonimiseerd (alleen scores en algemene statistieken blijven bewaard).

1.5 Technische loggegevens

- Welke gegevens: IP-adres, browser- en apparaatgegevens (user agent), besturingssysteem, tijdstempel van inlog- en gebruiksacties, foutmeldingen en serverlogs.
- Doel: beveiligen van het platform, opsporen van misbruik (bijvoorbeeld brute-force aanvallen) en analyseren van technische fouten.
- Grondslag: gerechtvaardigd belang (beveiliging en goede werking van het platform).
- Opslaglocatie: Firebase Hosting logs en Cloud Functions logs (EU/VS).
- Toegang: uitsluitend voor het beheer en ontwikkelaars die debugging uitvoeren.
- Beveiligingsmaatregelen:
  - Logs zijn alleen toegankelijk via accounts met rolgebaseerde rechten.
  - Loggegevens worden automatisch verwijderd na de bewaartermijn.
  - Logs bevatten geen inhoud van lessen of gebruikersinvoer, alleen technische metadata.
- Bewaartermijn: maximaal 90 dagen, daarna automatische verwijdering.
- Contact: bij vragen of verzoeken over logging kan men terecht bij support: lucas@codeblocks.nl

1.6 Feedback

- Welke gegevens: ingevulde feedbacktekst, score/rating, en eventueel naam en e-mailadres (optioneel veld).
- Doel: verzamelen van meningen en ervaringen om lessen, software en demo’s te verbeteren.
- Grondslag: toestemming van de gebruiker bij het invullen van het feedbackformulier.
- Opslaglocatie: Firestore database (EU/VS).
- Toegang: uitsluitend voor het beheer en het team onderwijsontwikkeling.
- Beveiligingsmaatregelen:
    - Alleen noodzakelijke gegevens worden opgeslagen; naam en e-mail zijn optioneel.
    - Toegang tot feedback is beperkt tot betrokken medewerkers.
    - Gegevens worden niet gedeeld met derden buiten noodzakelijke verwerkers (zoals Firebase/Google).
- Bewaartermijn: maximaal 6 maanden, waarna feedback wordt verwijderd of geanonimiseerd voor interne rapportages.
- Contact: bij vragen of verzoeken kan men terecht bij support: koen@codeblocks.nl.

1.7 Media en beeldrecht

- Welke gegevens: foto’s, video’s en eventueel namen van leerlingen of vrijwilligers die deelnemen aan lessen, demo’s of evenementen.
- Doel: promotie en verslaglegging van Codeblocks-activiteiten via de website, sociale media en drukwerk.
- Grondslag: expliciete toestemming van de betrokkene of, indien jonger dan 16 jaar, van de ouder/verzorger.
- Opslaglocatie: Google Drive (EU/VS) en op de Codeblocks-website en sociale mediakanalen.
- Toegang: uitsluitend voor het beheer en het communicatieteam.
- Beveiligingsmaatregelen:
    - Foto’s en video’s worden alleen gebruikt met toestemming.
    - Gegevens worden niet langer openbaar gehouden dan noodzakelijk.
    - Toestemming kan altijd worden ingetrokken; materiaal wordt dan verwijderd.
- Bewaartermijn: zolang het materiaal relevant is voor promotie of verslaglegging. Indien toestemming wordt ingetrokken, wordt het materiaal direct verwijderd.
- Contact: voor vragen of verzoeken kan men terecht bij support: lucas@codeblocks.nl.

1.8 Cookies en analytics

- Welke gegevens: cookie-ID, voorkeuren (bijv. gekozen taal of thema), cookie-toestemming (opt-ins), en – indien analytics actief – geanonimiseerde gebruiksstatistieken zoals bezochte pagina's en sessieduur.
- Doel:
  - Functionele cookies: zorgen dat de website correct werkt (bijv. sessiebehoud, thema-instellingen).
  - Analytische cookies: inzicht krijgen in gebruik van de website en zo de werking verbeteren.
  - Toestemmingscookies: onthouden welke cookie-instellingen een gebruiker gekozen heeft.
- Grondslag: toestemming via de cookiebanner (behalve strikt noodzakelijke cookies).
- Opslaglocatie: in de browser van de gebruiker, en bij gebruik van externe analytics-tools (bijv. Google Analytics) op hun servers (EU/VS).
- Toegang: uitsluitend voor het beheer; bij gebruik van externe tools ook de betreffende dienstverlener.
- Beveiligingsmaatregelen:
  - Alleen geanonimiseerde gegevens voor analytics.
  - Cookievoorkeuren zijn op elk moment aanpasbaar via de cookiebanner.
  - Geen tracking of marketingcookies zonder expliciete opt-in.
- Bewaartermijn:
  - Functionele cookies: zolang de sessie duurt of enkele dagen/weken voor instellingen.
  - Analytics-cookies: maximaal 13 maanden.
  - Toestemmingscookies: maximaal 12 maanden.

1.9 Beveiligingsincidenten

- Welke gegevens: registraties van incidenten, waaronder datum en tijdstip, aard van het incident, betrokken systemen en persoonsgegevens, aantal betrokken personen, en de getroffen maatregelen.
- Doel: voldoen aan de wettelijke verplichting om beveiligingsincidenten en datalekken te registreren, en verbetermaatregelen vast te leggen.
- Grondslag: wettelijke verplichting onder de AVG.
- Opslaglocatie: intern logboek (Google Drive of Firestore, beveiligd en alleen toegankelijk voor geautoriseerde accounts).
- Toegang: uitsluitend voor het beheer en de privacy-verantwoordelijke(n).
- Beveiligingsmaatregelen:
  - Incidentmeldingen worden centraal bijgehouden in een beveiligd logboek.
  - Alleen geautoriseerde personen mogen incidenten registreren en bekijken.
  - Incidenten worden geëvalueerd om herhaling te voorkomen.
- Bewaartermijn: minimaal 2 jaar, zodat incidenten ook later nog kunnen worden geanalyseerd of aangetoond bij een controle.

2. Datalekprocedure

2.1 Doel

Deze procedure beschrijft hoe Codeblocks omgaat met beveiligingsincidenten en datalekken. Het doel is schade voor betrokkenen te beperken, te voldoen aan de meldplicht onder de AVG en herhaling te voorkomen.

2.2 Definitie datalek

Een datalek is iedere inbreuk op de beveiliging waardoor persoonsgegevens:

- verloren zijn gegaan,
- toegankelijk zijn voor onbevoegden,
- gewijzigd of vernietigd zijn,
- of onrechtmatig zijn verstrekt.

Voorbeelden:

- Laptop of telefoon met toegang tot persoonsgegevens raakt kwijt of wordt gestolen.
- Een e-mail met persoonsgegevens wordt naar een verkeerde ontvanger gestuurd.
- Onbevoegden krijgen toegang tot een Firebase-account.
- Firestore-data wordt per ongeluk publiek gezet.

2.3 Rollen en verantwoordelijkheden

- Meldpunt datalekken: support via Lucas@codeblocks.nl.
- Privacy lead (beheer): beoordeelt het incident, bepaalt de ernst en of melding noodzakelijk is.
- Beheer: zorgt voor technische maatregelen (bijv. reset accounts, sluiten database).
- HR / communicatie: indien nodig betrokken bij informeren van vrijwilligers of scholen.

2.4 Stappenplan bij incident

1. Melden
    - Elk vrijwilliger of betrokkene die een mogelijk datalek ziet, meldt dit direct via koen@codeblocks.nl.
2. Registreren
    - Het incident wordt vastgelegd in een intern logboek met:
        - Datum en tijd
        - Naam melder
        - Beschrijving incident
        - Betrokken gegevens en systemen
        - Aantal betrokken personen
3. Beoordelen (binnen 24 uur)
    - De privacy lead beoordeelt de ernst van het incident:
        - Welke soort gegevens zijn gelekt (bijv. e-mail vs. leerlingresultaten)?
        - Hoeveel personen zijn getroffen?
        - Zijn de gegevens herleidbaar naar een persoon?
        - Kan er schade ontstaan (identiteitsfraude, reputatie, verlies van controle)?
4. Beslissen melding Autoriteit Persoonsgegevens (binnen 72 uur)
    - Indien er sprake is van een risico voor betrokkenen, wordt melding gedaan bij de AP.
    - Deze melding bevat: aard incident, aantal betrokkenen, categorie gegevens, getroffen maatregelen.
    - Als er géén risico is → alleen registreren in logboek.
5. Informeren betrokkenen (indien nodig)
    - Als er waarschijnlijk een groot risico is voor betrokkenen, worden zij direct geïnformeerd per e-mail.
    - In deze melding staat: wat er is gebeurd, welke gegevens het betreft, wat de risico’s zijn, en welke maatregelen zijn genomen.
6. Herstel en maatregelen
    - Technische maatregelen: bv. accounts resetten, database afsluiten, IP blokkeren.
    - Organisatorische maatregelen: extra training vrijwilligers, aanpassen procedures.
7. Evalueren en afsluiten
    - Incident wordt nabesproken en geëvalueerd.
    - Logboek wordt aangevuld met: genomen acties, eventuele melding bij AP, lessons learned.

2.5 Bewaartermijn incidenten

- Incidenten worden minimaal 2 jaar bewaard in het logboek, zodat herhaling kan worden voorkomen en bij controles aangetoond kan worden hoe er is gehandeld.