Unilogin

Formål

Unilogin er et webbaseret digitalt id for elever, forældre, og medarbejdere på institutioner på dagtilbudsområdet og undervisningsområdet. Unilogin giver adgang til nationale tjenester og en lang række pædagogiske services - f.eks. online læremidler.

Styrelsen for It og Læring stiller som databehandler den digitale identifikationsløsning Unilogin til rådighed for institutionerne på undervisningsområdet og dagtilbudsområdet til brug for styring af elevers, forældres og medarbejderes adgangsrettigheder til pædagogiske og administrative tjenester. Styrelsen for It og Lærings behandling består i at opbevare personoplysninger i Unilogins Skolegrunddata samt at give private leverandører af digitale læremidler og værktøjer adgang til personoplysninger i Unilogins Skolegrunddata efter dokumenteret instruks fra den dataansvarlige via en af de webgrænseflader som styrelsen stiller til rådighed for den dataansvarlige.

Unilogin bruges som identifikationsløsning ved en lang række digitale tjenester på undervisningsområdet, såsom de nationale test, Undervisningsministeriets digitale prøveafviklingssystem, de nationale trivselsmålinger m.v. Endvidere bruges Unilogin i institutionernes egne lokale løsninger, såsom digitale læremidler og digitale lærings- og samarbejdsløsninger.

Da Unilogins Skolegrunddata anvendes til styring af adgangsrettigheder – f.eks. i forbindelse med digitale prøver – er det vigtigt, at der kan ske en entydig identifikation af den pågældende bruger.

Hjemmel for Styrelsen for It og Lærings databehandling

Hjemler for anvendelse af Unilogin som adgangsmiddel og uden at der sker videregivelse til Styrelsen for It og Læring findes i:

Bekendtgørelse af lov om kommunal indsats for unge under 25 år (LBK nr 1301 af 04/09/2020): Unilogin anvendes til brug for styring af adgangsrettigheder til pædagogiske og administrative tjenester for brugere og medarbejdere. Styrelsen for It og Læring handler efter instruks fra kommunerne eller de selvejende institutioner. Styrelsen for It og Læring skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, og mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelseslovgivningen. Styrelsen for It og Læring skal også sikre, at Unilogin opfylder kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i databeskyttelsesforordningen.

Styrelsen for It og Læring får videregivet data til egne formål. Opgaven og videregivelsen har hjemmel i følgende love og administrative forskrifter med det heri angivne formål:

Bekendtgørelse om obligatoriske test i folkeskolen i skoleårene 2022/23 til og med 2025/26 (Folkeskolens Nationale Overgangstest) (BEK nr 1223 af 31/08/2022): Unilogin anvendes som adgangsmiddel til Undervisningsministeriets digitale test- og prøveafviklingssystem, herunder testresultater, i forbindelse med de nationale test. Undervisningsministeriet opbevarer data fra Unilogin i 'Test- og Prøvesystemet' med henblik på at foretage analyser og udarbejde rapporter over den enkelte skoles testresultater set i forhold til det samlede landsresultat. Heri skal indgå en vurdering af skolens testresultater set i forhold til elevernes sociale baggrund

Bekendtgørelse om folkeskolens prøver (prøvebekendtgørelsen) (BEK nr 1224 af 31/08/2022): Unilogin anvendes som adgangsmiddel til Undervisningsministeriet selvrettende system 'Test og Prøvesystemet' i forbindelse med folkeskolens afgangsprøver.

Bekendtgørelse om måling af elevernes trivsel i folkeskolen (BEK nr 525 af 01/05/2019). De nationale trivselsmålinger skal foretages via et trivselsmålingsværktøj som Styrelsen for It og Læring stiller til rådighed. Adgangen til trivselsmålingsværktøjet sker ved at logge på med Unilogin. Styrelsen for It og Læring kobler elevens Unilogin sammen med elevens trivselsmåling i forbindelse med forskning i udviklingen af elevernes trivsel. Unilogin anvendes heri kun til statistiske og videnskabelige formål og ikke administrativt over for eleven

Dataansvarlig myndighed
Uddannelsesinstitutioner og kommuner

Databehandler

Styrelsen for It og Læring

STILs underdatabehandler - udvikling

Nine

STILs underdatabehandler – drift, vedligehold

Statens It (SIT) leverer infrastrukturen til STILs datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

Kategorier af registrerede og kategorier af personoplysninger, der behandles i systemet

Der behandles personoplysninger om elever, kontaktpersoner og medarbejdere i statsinstitutioner, kommuner, regioner og selvejende institutioner på dagtilbudsområdet og undervisningsområdet.

De personoplysninger, der behandles i Unilogin er CPR-nummer, navn, adresse, telefonnummer, email, uddannelsesoplysninger og kontaktpersonstatus samt oplysninger om roller og relation.

Der behandles ikke følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9.

Hvor længe opbevares personoplysninger i systemet?

De dataansvarlige har ansvaret for at vedligeholde oplysninger i Unilogin, herunder sletning af personoplysninger, når en elev eller medarbejder ikke er tilknyttet institutionen.

Af hensyn til evt. skoleskift opbevares UniID og CPR-nummer i 12 måneder, men den tidligere institution har ikke adgang til disse oplysninger. Det sikrer, at eleven kan få
samme Unilogin brugernavn på den nye institution. Alle øvrige personoplysninger slettes i Unilogin, så snart institutionen sletter dem fra deres studieadministrative systemer.

Brugere i SkoleGrunddata, som ikke i 12 måneder har haft tilknytning til en institution, slettes. Ved tilknytning forstås, at brugeren er importeret til SkoleGrunddata fra et administrativt system. Brugerens institutionstilknytning kan fjernes (institutionen
nedlægges eller brugeren slettes i institutionens import). Derved har brugeren ingen institutionstilknytning. Brugere, som udelukkende er oprettet fordi de er kontakt til en eller flere elever, slettes straks efter at den sidste elev, de er kontakt for, ikke længere er tilknyttet en institution.
Sletning medfører at alle data slettes permanent fra SkoleGrunddata. Unilogin brugerID (UniID) fra en slettet bruger kan ikke genbruges.

Som levn fra en fjernet funktionalitet findes der brugere med rettighed til hjælpesystemet ElevAdgang som er administrator. Der er p.t. ikke en slettepolitik for denne gruppe, og sletning varetages af STIL support på den dataansvarlige instruks som en manuel opgave.

Hvor stammer oplysningerne fra?

Personoplysninger i Unilogin indtastes af en brugeradministrator hos den dataansvarlige. Indtastningen sker i den dataansvarliges studieadministrative system, som overfører personoplysningen til Unilogins Skolegrunddata.
Hvis data hentes i CPR i det studieadministrative system påføres dette i importen til Unilogins Skolegrunddata. Ændres der i data efter CPR-opslaget påføres denne oplysning også. Unilogins Skolegrunddata foretager ikke kontrol af disse oplysninger.

Hvem har adgang til at se og behandle persondata i systemet?

Brugeradministratorer hos den dataansvarlige har adgang til at indtaste, korrigere og slette personoplysninger. Den registrerede kan selv se sine oplysninger, sine adgange via Mit UNI-Login og hvem den registrerede er kontaktperson for. Den registrerede kan selv skifte sin adgangskode.

Modtagere

Styrelsen for It og Læring giver adgang til de dataansvarliges øvrige databehandlere efter dokumenteret instruks fra de dataansvarlige via en af de grænseflader, som styrelsen stiller til rådighed. Dette sker gennem systemet Tilslutning, hvor der ikke behandles persondata.

Styrelsen for It og Læring får data i Unilogin videregivet til egne formål som beskrevet i de oven for nævnte lovhjemler og til de oven for nævnte formål samt til statistiske og videnskabelige formål.

Styrelsen for It og Læring videregiver oplysninger i Unilogin til forskere og forskningsinstitutioner til brug for deres forskningsprojekt på baggrund af ansøgninger om udtræk herom. Udtrækket sker gennem STILs forskerkonti hos Danmarks Statistisk.

Sker der overførsler til tredjelande eller internationale organisationer?

Ja	
Nej	

Bemærkninger til overførsler til tredjelande eller internationale organisationer

Styrelsen for It og Læring overfører ikke personoplysninger i Unilogin til tredjelande eller internationale organisationer.

Overførsler til tredjelande kan potentiel forekomme, såfremt en dataansvarlige giver styrelsen instruks om, at give en privat leverandør adgang til personoplysninger i Unilogin og denne private leverandør befinder sig i et tredjeland eller har en underdatabehandler, som befinder sig i et tredjeland. I så fald fører den dataansvarlige egen fortegnelse over sådanne overførsler og sikrer, at der foreligger et gyldigt overførselsgrundlag.

Generelle sikkerhedsforanstaltninger

Styrelsen for It og Læring autoriserer adgang for de personer i styrelsen, der har et arbejdsbetinget behov for at kunne tilgå personoplysninger i systemet. Styrelsen fører regelmæssig kontrol med, at kun personer med arbejdsbetinget behov kan tilgå personoplysninger i systemet. Styrelsen lukker straks en medarbejders adgang til oplysningerne, hvis autorisationen fratages eller udløber. Styrelsen for It og Læring sikrer, at disse personer har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
Som ansvarlig myndighed for systemet er Styrelsen for It og Læring ansvarlig for at iagttage kravet i databeskyttelsesforordningens artikel 32 om behandlingssikkerhed. Styrelsen foretager en risikovurdering og gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder blandet andet, alt efter hvad der er relevant, kryptering og logning.

Fastsættelsen af de omhandlede foranstaltninger sker under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder. Styrelsen for It og Læring sørger som minimum for at iværksætte følgende sikkerhedsforanstaltninger:

1) Styrelsen fastsætter interne retningslinjer for informationssikkerhed, herunder retningslinjer for organisatoriske forhold, logisk og fysisk sikring, herunder administration af adgangskontrolanordninger og autorisationsanordninger samt kontrol af autorisationer. Styrelsen instruerer de autoriserede medarbejdere i reglerne om interne arbejdsgange og sikkerhedsforanstaltninger, herunder sikkerhedsforanstaltninger ved evt. anvendelse af hjemmearbejdsplads og mobilt udstyr.

2) Styrelsen anvender et almindeligt anerkendt standardrammeværktøj, såsom ITIL, til at understøtte stabil og sikker drift.

3) Styrelsen etablerer et informationssikkerhedsledelsessystem baseret på ISO27001-standarden, herunder en it-sikkerhedspolitik, områdepolitikker, passende kontroller samt relevante retningslinjer og procedurer i forhold til informationssikkerheden.