Ansvarig enhet
Universitetskansliet

Datum
2018-05-14

Dnr
LTU-1175-2018

Beslutsfattare: Rektor	Beslutsdatum: 2018-05-14
Dokumenttyp: Riktlinjer	Träder i kraft: 2018-05-14
Giltighetstid: tillsvidare	Bör uppdateras före: 2019-05-14

Riktlinjer för testmiljöer

1. Inledning och syfte.

General Data Protection Regulation (GDPR) är en dataskyddsförordning som beslutades av EU under år 2016 och som ersätter den svenska personuppgiftslagen (PUL). GDPR med träder i kraft som svensk lagstiftning den 25 maj 2018.

Syftet med dessa riktlinjer är att ge vägledning för hur personuppgifter i testdata ska hanteras i de testmiljöer som finns på universitetet samt att säkerställa att behandlingen av personuppgifterna

2. Testmiljöernas syfte och utbredning

Universitetet har ett antal testmiljöer i syfte att testa funktionalitet i IT-stöd inför nya releaser av befintliga IT-stöd, men även vid införandet av helt nya. Tesmiljöerna finns antingen hos ITS, ute i verksamheten eller hos externa leverantörer (personuppgiftsbiträden). Oavsett testmiljöns lokalisering gäller samma riktlinjer och förhållningssätt.

3. Testmiljöernas innehåll

3.1 Allmänt

Testmiljöerna kan innehålla personuppgifter avseende *Studenter, Anställda, Leverantörer* eller *kunder.* När det gäller leverantörer och kunder är det i första hand personuppgifter till kontaktpersoner, men i enstaka fall förekommer även enskilda firmor och då identifieras de med personnummer

3.2 Huvudregel för användning av personuppgifter i testmiljöer

Användning av personuppgifter i testmiljöer ska som huvudregel ske med utvecklarnas egna identiteter eller med påhittade identiteter fram till dess att ett system ska tas i produktion.

För tester med personnummer kan Skatteverket på begäran tillhandahålla personnummerserier som inte är kopplade till verkliga personer (s.k. testpersonnummer). Det går även att använda personnummer som inleds med ett tidigare århundrande, t.ex. ”17YYMMDDXXXX”.

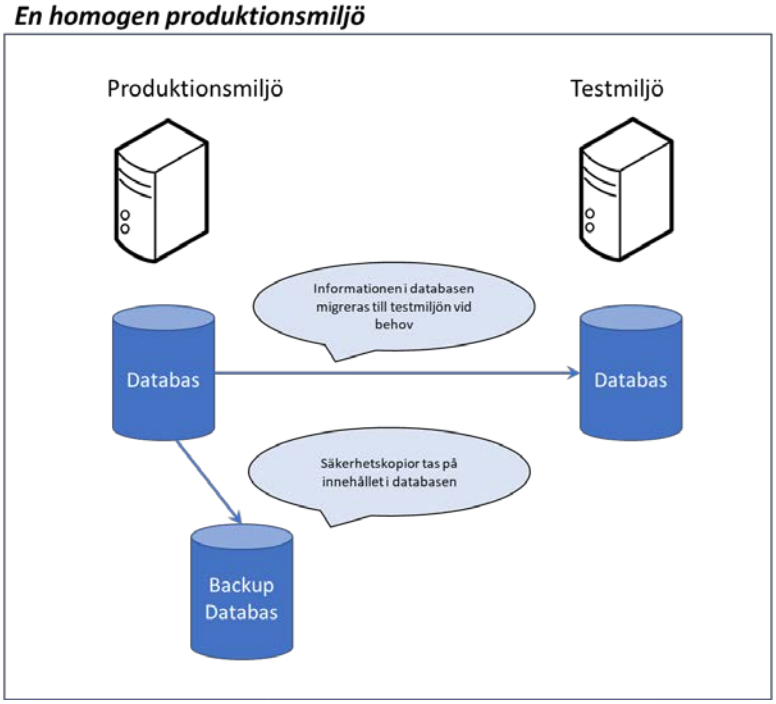
Villkoret är att checksiffran (sista siffran) måste stämma. Observera dock att ett sådant personnummer inte kan verifieras mot befolkningsregistret. Sådana personnummer går att hämta på följande adress:
https://oppnadata.se/datamangd/#esc_entry=65411&esc_context=6

I de fall andra personnummer än påhittade eller utvecklarnas egna måste användas, ska de hanteras i enlighet med avsnitt 4 i denna riktlinje.

3.3 Förhållningssätt

Förhållningssättet är att en applikation eller ett system består av en homogen miljö bestående av ett antal enheter och företeelser såsom produktionsmiljö (produktionsdator och i vissa fall en standby), databas, backuper av databasen samt i vissa fall även en eller flera testmiljöer och utbildningsmiljöer med tillhörande databas.

Syftet med hela testmiljön är att säkerställa systemets funktion och därmed säkra ändamålet med behandlingen av personuppgifter. Ett exempel är att kunna säkra löneutbetalningar till anställda (*se bild nedan*)



4. Uppgiftsminimering och pseudonymisering

Personuppgifter ska i samtliga fall *minimeras* så att endast de absolut nödvändigaste personuppgifterna finns med för att kunna testa avsedd funktionalitet utan att göra avkall på kvaliteten i testerna. I de fall som testdatat måste innehålla *extra skyddsvärda* eller *känsliga personuppgifter* ska en RSA (Risk- och sårbarhetsanalys) utföras för respektive applikation/system. Resultatet av RSA kan, men behöver inte, innebära att personuppgifterna måste *pseudonymiseras* eller maskeras på ett sådant sätt att en specifik nu levande person inte identifieras.

4.1 Pseudonymisering

Dataskyddsförordningens definition av pseudonymisering är följande: ”Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.”

4.2 Överföring av testdata

Överföring av testdata till testmiljöer från exempelvis produktionsmiljöer ska ske på ett IT-säkerhetsmässigt sätt. Resultatet av en RSA kan, men behöver inte, innebära att personuppgifter måste *pseudonymiseras* eller maskeras på ett sådant sätt att en specifik nu levande person inte identifieras.

4.3 Radering

Efter avslutade tester och/eller då behovet av testdatat inte längre finns, ska personuppgifterna utan dröjsmål raderas bort. Hur länge uppgifterna får finnas kvar är beroende av hur ofta testerna körs och hur komplext det är att ta bort testdatat. Rimlighetsprincipen får styra tidsaspekten.

4.4 Behörigheter

Behörighet till testmiljöerna ska begränsas till ett fåtal användare och behörigheterna ska tas bort utan dröjsmål när en användare inte längre är i behov av att komma åt respektive tesmiljö. Samma princip gäller för användare vars syfte är att utföra utbildning i en utbildningsmiljö.

4.5 Personuppgiftsbiträden

I de fall som ett personuppgiftsbiträde anlitas för testverksamheten måste ett personuppgiftsbiträdesavtal upprättas.

4.6 Rättslig grund för behandlingen

Den rättsliga grunden för behandlingen är *myndighetsutövning*.