

Checklista vid upphandling av digital forskningspersonsplattform (system för digital insamling av samtycken och självrapporterade forskningsdata)

Stöd för kravställning vid lärosäten och regioner

Vad avser checklistan?

En forskningspersonsplattform är ett system som identifierar forskningspersonen med e-legitimation, informerar och inhämtar samtycke, kommunicerar säkert i två riktningar, samlar in självrapporterade data med bibehållen identitetskoppling, och möjliggör registerlänkning och återkontakt. Checklistan nedan avser kravställning av just den typen av system, Verified Participant Data Capture (VPDC) – till skillnad från renodlade Electronic Data Capture (EDC)-system, där data matas in av personal och inte av forskningspersonen själv.

Teckenförklaring

Varje punkt är märkt med vem den huvudsakligen berör: [D] Dataskyddsombud/motsvarande funktion, [F] Forskare/studiepersonal, [P] Deltagaren (forskningspersonen). Flera märkningar betyder att flera roller berörs. Märkningen är ett stöd för att snabbt se vem i organisationen som behöver involveras i svaret – inte en begränsning av vem som får ställa frågan.

Varför nu?

Integritetsskyddsmyndigheten (IMY) har i ett förhandssamråd om en stor svensk befolkningsstudie (dnr IMY-2026-8907, 2026-06-24) gjort bedömningar som direkt påverkar hur digitala forskningspersonsplattformar (samtyckes- och enkätssystem) bör kravställas:

- Känsliga personuppgifter för forskning är information i högsta säkerhetsklass, där K (konfidentialitet) = 3 och R (riktighet) = 3, medan T (tillgänglighet) kan vara lägre.
- För K = 3 när känsliga personuppgifter samlas in direkt från deltagare måste 2-faktor-autentisering användas. Lämpliga metoder är e-legitimation (BankID eller Freja eID+). Token-länkar via e-post uppfyller inte lärosätens egna krav på stark autentisering.
- För R = 3 kan endast e-legitimation i dagsläget verifiera vem som faktiskt svarar, vilket är en förutsättning för riktighetsprincipen (art. 5.1 d) och därmed för t ex länkning av självrapporterade data mot nationella register via personnummer.

IMY påpekade också att riskreducerande åtgärder i konsekvensbedömningar ofta enbart täcker behandlingen efter insamlingen, medan själva insamlingsfasen – där de känsliga uppgifterna skapas – lämnas oskyddad. Såväl insamling av samtycke som insamling av självrapporterade data till forskningsstudier innebär hantering av känsliga personuppgifter. Checklistan nedan är indelad i samtyckeshantering (del A) och datainsamling (del B), med gemensamma krav i del C.

Varför en forskningspersonsplattform?

Nytta för forskaren och DSO. En sammanhållen forskningspersonsplattform ersätter lösryckta token-länkar och manuell pappershantering med en regelefterlevande process genom hela kedjan, från samtycke till uppföljning. Det minskar det egna arbetet med att bygga och underhålla säkerhetslösningar kring insamlingsfasen, och ger färdig dokumentation att luta sig mot i konsekvensbedömningen.

Nytta för deltagaren. Med en enda stark inloggning (SSO) via BankID eller Freja eID+ får deltagaren en gemensam ingång till samtycke, enkäter, kommunikation och egna resultat — istället för att logga in med olika metoder i olika delsystem. Det förenklar deltagandet och ger samtidigt en stark garanti för att det verkligen är rätt person som lämnar och tar emot uppgifterna.

Ekonomiska fördelar. En sammanhållen forskningspersonsplattform minskar den administrativa bördan kring pappershantering, manuell identitetskontroll och uppföljning av flera separata system.

Digitalisering och integrationsmöjligheter. Ett system byggt med öppna gränssnitt (API:er) öppnar för att koppla samman samtycke, enkätdata och andra forskningssystem över tid — och för framtida integrationer med exempelvis kvalitetsregister, biobanker och journalsystem, i den takt verksamheten är redo för det.

Del A. Forskningspersonsinformation och samtycke

1. Laglig grund, dataskydd och informationssäkerhet

☐ [D] Laglig grund för personuppgiftsbehandlingen

Kan leverantören säkerställa att all personuppgiftsbehandling har en tydligt dokumenterad laglig grund?

☐ [D,F] Dataminimering

Möjliggör systemet effektiv dataminimering så att endast absolut nödvändiga uppgifter samlas in och endast visas för de roller som behöver se dem?

☐ [D] Lagring av data

Lagras all data inom Sverige/EU, med full transparens kring vilka underbiträden som används?

☐ [D] Transport av data

Hanteras all data på ett säkert sätt både vid överföring och vid vila (lagring)?

☐ [D] Separation av identitet och innehåll

Lagras identifierande uppgifter i annan databas än de hälsouppgifter deltagaren rapporterar, så att ett intrång inte röjer båda? [1]

☐ [D] Personuppgiftsbiträdesavtal och incidenthantering

Finns färdiga PUB-avtal, dokumenterade rutiner för incidentrapportering inom 72 timmar och stöd vid anmälan till IMY?

☐ [D] Klassning

Stödjer systemet verksamhetens specifika krav på informationsklassning (t.ex. KRT 3:3:1) i hela kedjan — inklusive insamlingsfasen?

☐ [D,F] Långtidsarkivering

Går data att exportera i ett format som möjliggör långtidsarkivering med bibehållen signatur?

2. Identifikation och signering

☐ [F,D] Hur säkerställs att rätt person signerar?

Använder systemet e-legitimation (t.ex. BankID) för att säkerställa identiteten? [2,3]

☐ **[F,D] Hur säkerställs att rätt vårdnadshavare signerar?**

Finns tekniskt stöd via realtidskontroll mot folkbokföringsregistret, och krävs samtliga vårdnadshavares signatur för att samtycke för minderårig ska vara giltigt? [2]

☐ **[F] Kontrasignering vid GCP-studier**

Säkerställer systemet att signaturer sker i rätt ordning (deltagare före provare), i samma session och med korrekt tidsstämpling, där även provaren signerar med e-legitimation (BankID)? [2,3]

☐ **[F] Förhindra att deltagare samtycker flera gånger**

Finns en dubblettkontroll som förhindrar samma individ från att samtycka till samma studie flera gånger? [1]

☐ **[F,D] Registrering av manuella samtycken**

Kan pappersbaserade samtycken föras in i samma databas, så att studien har en komplett och spårbar samtyckesöversikt? [2]

3. Regulatoriska frågor och spårbarhet

☐ **[D,F] Versionshantering av samtycken**

Finns robust och spårbar versionshantering av exakt vilken version av forskningspersonsinformation en person godkänt, och förhindras signering av icke-giltiga versioner? [3]

☐ **[D] Audit trail**

Genererar systemet en sökbar och oföränderlig händelselogg för alla ändringar och åtkomster?

☐ **[F] Monitorering**

Erbjuder systemet verktyg för provare och monitorer att på distans granska och följa upp samtycken och inklusionstakt? [3]

☐ **[F,D] Validering enligt bransch- och myndighetsstandard**

Är systemet kvalitetssäkrat och dokumenterat enligt GAMP 5, ICH E6 (GCP), FDA 21 CFR Part 11 och EudraLex Annex 11? [2]

☐ **[F] Decentraliserad inklusion**

Stödjer systemet inklusion på distans, t.ex. vid videobesök, utan att signeringskedjan bryts? [3]

4. Deltagarens rättigheter över tid (dynamiskt samtycke)

☐ **[P] Insyn i eget samtycke**

Kan deltagaren själv logga in och läsa, ladda ner och skriva ut sitt signerade samtycke? [2]

☐ **[P,D] Återkallelse**

Kan deltagaren enkelt återkalla samtycket, med dokumenterad tidpunkt och genomslag i studiens övriga system? [2,4]

☐ **[F,D] Förnyat samtycke**

Kan systemet inhämta nytt samtycke vid uppdaterad information eller ny delstudie, utan att tidigare samtycken skrivs över? [3]

☐ **[P,D] Information och kontaktpunkt**

Presenteras lättbegriplig information om behandlingen och om hur rättigheterna utövas vid insamlingstillfället, och finns en tydlig kontaktpunkt för frågor? [2]

☐ **[D,F] Giltigt samtycke vid varje tillfälle**

Kontrollerar systemet automatiskt att samtycket fortfarande är giltigt – inte återkallat eller ersatt av en nyare version – innan studiemoment genomförs (t.ex. en enkät visas eller påminnelse skickas)?

5. Inkludering och tillgänglighet

IMY:s krav på e-legitimation som primär autentiseringsmetod innebär inte per automatik en risk för att utesluta grupper som saknar BankID eller Freja eID+ förutsatt att systemet erbjuder dokumenterade alternativa vägar. Den här sektionen säkerställer det.

☐ [P,F] Alternativ för den som saknar e-legitimation

Finns dokumenterade alternativa vägar (t.ex. pappersblankett eller assisterad inklusion) som registreras i samma databas? [2]

☐ [F] Täckningsgrad i målpopulationen

Kan leverantören redovisa underlag för hur stor andel av den avsedda populationen som kan använda den valda identifieringsmetoden? [2,4]

☐ [P] Begriplighet och stöd

Finns pedagogiskt stöd (t.ex. korta filmer, texter anpassade för barn och unga, vanliga frågor) och möjlighet att få hjälp av studiepersonal? [1,2]

☐ [P] Digital tillgänglighet

Uppfyller gränssnittet krav på tillgänglighet (WCAG/DOS-lagen) och fungerar det på mobil, tablet och dator? [1]

Del B. Insamling av självrapporterade data (enkäter, ePRO)

6. Stark autentisering av deltagaren, inte bara av personalen

☐ [D,P] Stark autentisering även för respondenten

Krävs e-legitimation (t.ex. BankID) också av den som besvarar enkäten – inte enbart av forskare och studiepersonal? Detta är den punkt där etablerade EDC- och ePRO-system oftast brister. [1,4]

☐ [D] Länkar i e-post och SMS

Undviker lösningen att känslig insamling görs åtkomlig via token-länkar i e-post eller SMS, som kan följas av var och en med åtkomst till brevlådan?

☐ [P] Säker återupptagning

Kan deltagaren avbryta och återupptaga ett pågående ifyllande genom ny stark autentisering, utan att en sparad session kan kapas?

☐ [P,D] Sessionshantering

Kan deltagaren se och avsluta aktiva sessioner på andra enheter, och sker automatisk utloggning vid inaktivitet? [1]

☐ [D,P] Skydd av data på deltagarens enhet

Krypteras lokalt lagrade data på deltagarens enhet, med nyckelhantering som gör data oåtkomliga om enheten försvinner? [1]

☐ [D] Klassningen måste hålla i insamlingsfasen

Motsvarar autentiseringen verksamhetens egen informationsklassning (2FA på BankID-nivå) i det ögonblick de känsliga uppgifterna skapas – och inte bara när de lagras?

7. Riktighet, identitetsbindning och registerlänkning

☐ [D,F] Vem lämnade svaren?

Kan systemet i efterhand styrka vilken fysisk person som lämnat varje enskilt svar (riktighetsprincipen, art. 5.1 d)?

☐ **[F,D] Länkning till personnummer**

Är identiteten verifierad på ett sätt som medger länkning till nationella hälsodataregister, kvalitetsregister och biobanksdata utan risk för felaktig attribuering? [1]

☐ **[F,P] Återkontakt vid fynd**

Går det att med säkerhet återkontakta rätt individ om studiedata föranleder det, t.ex. vid kliniskt relevanta fynd?

☐ **[F,D] Samma person genom hela studien**

Säkerställs att den som signerat samtycket är samma person som besvarar enkäter, lämnar prover och tar del av återkopplade resultat? [4]

☐ **[D] Riskreducering i själva insamlingsfasen**

Kan leverantören redovisa vilka riskreducerande åtgärder som gäller specifikt under insamlingen – underlag som behövs i verksamhetens konsekvensbedömning?

8. Instrument, datakvalitet och datatyper

☐ **[F] Validerade instrument**

Finns ett bibliotek av etablerade PROM (t.ex. EQ-5D-5L, RAND-36) med korrekt poängberäkning och stöd för licenshantering? [1,4]

☐ **[F,P] Deltagarstyrd rapportering**

Kan deltagaren rapportera symtom som inte finns i en förvald lista, med fritext och skattningsskalor? Självdefinierade symtom och fritextrapportering blir allt vanligare och uppfattas som viktigt av studiedeltagare. [1]

☐ **[F] Nya datatyper**

Stöds datatyper som inte kan samlas in på papper, t.ex. tredimensionella symtomritningar och grafisk återkoppling av egen utveckling över tid? [1,4]

☐ **[F] Kvalitetskontroller**

Finns logiska kontroller, hoppregler, obligatoriska respektive frivilliga fält och möjlighet att spara ofullständiga svar och fortsätta senare? [1]

☐ **[F] Bortfallsuppföljning**

Kan svarsfrekvens och bortfall följas i realtid per instrument, tidpunkt och studiecenter?

9. Longitudinell insamling och följsamhet

☐ **[F] Scheman och påminnelser**

Kan schemalagd insamling med automatiska påminnelser konfigureras per delstudie, tidpunkt och instrument? [4]

☐ **[F,D] Långa uppföljningstider**

Kan deltagare följas i många år med bibehållen identitet, samtyckesstatus och versionshistorik? [3,4]

☐ **[P] Nytt för deltagaren**

Får deltagaren tillgång till sina egna data och visualiseringar — en faktor som gynnar långsiktig följsamhet och datakvalitet? [1]

☐ **[P,F] Närhet i tid, tidsstämpling, spontanrapportering**

Kan data rapporteras mellan de schemalagda tillfällena i nära i tid till upplevelsen, med korrekt tidsstämpling, för att minska minnesfel (recall bias)? [1,4]

10. Kommunikation och återkoppling

☐ [D,F] Stöd för att kommunicera säkert med deltagare

Finns inbyggt stöd för krypterad, individualiserad tvåvägskommunikation i systemet? [2]

☐ [D] Integritetssäker kommunikation

Förhindrar lösningen att känsliga uppgifter skickas via osäkra kanaler (e-post/SMS)?

☐ [F,P] Återkoppling av individuella resultat

Kan studien återkoppla individuella resultat (t.ex. provsvar) till deltagaren på ett identitetssäkert sätt? [4]

☐ [D,P] Verifierade kontaktvägar

Skickas inbjudningar och påminnelser på ett integritetssäkert sätt till kontaktvägar som deltagaren själv har valt och verifierat?

☐ [F,P] Rekrytering och studieerbjudanden

Kan intresserade skapa en profil för att få erbjudanden om studier de kan vara aktuella för? [2]

11. Integration, interoperabilitet och export

☐ [F,P] Samma identitet i alla systemdelar

Kan den starka identifieringen återanvändas för inloggning (SSO) i projektets övriga studiesystem, så att samtycke och enkätsvar hör till samma verifierade individ — och deltagaren bara behöver logga in en gång? [1]

☐ [F] API:er

Finns dokumenterade API:er för integration mot eCRF, enkätverktyg, genomikdatabaser och forskningsdataplattformar? [2]

☐ [D,F] Frågor om samtyckesstatus i realtid

Kan andra behöriga system i realtid fråga om giltigt samtycke finns för en viss individ och ett visst ändamål? [2]

☐ [F] Export till verksamhetens analysmiljö

Kan data exporteras i öppna format till lärosätets egen säkra analysmiljö (t.ex. REDCap) utan leverantörsberoende? [4]

☐ [F] Fristående komponenter

Kan enskilda delar av systemet (t.ex. bara samtyckesmodulen, eller bara enkätverktyget) användas fristående tillsammans med andra system, utan att kräva en total ersättning av befintlig infrastruktur?

☐ [D] Pseudonymisering och kodnyckel

Hanteras kodnyckeln separat från studiedata, och kan pseudonymiseringen dokumenteras så att den kan bedömas i konsekvensbedömningen? [4]

☐ [D] Bedömning av pseudonymiseringens tillräcklighet

Kan leverantören bistå med underlag för att bedöma om pseudonymiseringen — tillsammans med övriga skyddsåtgärder — räcker för en viss klassificering, även när ovanliga kombinationer av variabler skulle kunna göra enskilda indirekt identifierbara?

Del C. Krav på drift, förvaltning och dokumenterad erfarenhet

12. Drift, kontinuitet och avtalsfrågor

☐ [D] **Tillgänglighet och kontinuitet**

Finns SLA, redundans, backup och dokumenterad kontinuitetsplan, så att en pågående insamling inte avbryts? [1]

☐ [D] **Säkerhetstester**

Genomförs återkommande penetrationstester och sårbarhetsanalyser av oberoende part, och redovisas resultat och åtgärder för kunden?

☐ [D] **Ägande av data och immateriella rättigheter**

Är det avtalat att forskningshuvudmannen äger studiedata och samtycken? [2]

☐ [D] **Exit och dataportabilitet**

Vad händer vid avtalets slut – garanteras fullständig export i öppet format samt verifierad radering?

☐ [D] **Beroende av enskild leverantör**

Finns öppen källkod, standardiserade format eller andra åtgärder som begränsar inlåsnings effekter över en studies hela livslängd? [3]

13. Uppföljning, granskning och dokumenterad erfarenhet

☐ [D] **Stöd för uppföljning av konsekvensbedömning**

Bistår leverantören med underlag för verksamhetens skyldighet enligt art. 35.11 att regelbundet kontrollera att behandlingen sker i enlighet med konsekvensbedömningen och att se över om riskerna förändras?

☐ [D] **Underlag till konsekvensbedömningens omfattning**

Kan leverantören bistå med underlag om behandlingens omfattning (t.ex. antal registrerade, vilka roller/aktörer som har åtkomst, eventuell överföring till tredje part) till kundens systematiska beskrivning av behandlingen?

☐ [D] **Behörighetsstyrning och återkommande genomgång**

Finns rollbaserad behörighetsstyrning, loggning av åtkomst till känsliga fält och rutin för periodisk genomgång av behörigheter?

☐ [F] **Erfarenhet från skarpa studier**

Kan leverantören visa att systemet använts i etikprövade studier av relevant storlek och komplexitet – inklusive läkemedelsprövningar, befolkningsstudier och studier med vårdnadshavarsamtycke? [1,2,3,4]

☐ [F] **Referentgranskad dokumentation**

Är systemet och dess användning beskrivna i vetenskaplig, referentgranskad litteratur, så att funktion och begränsningar kan granskas oberoende? [1,2,3,4]

☐ [F,D] **Utvärderade begränsningar**

Redovisar leverantören även kända begränsningar (t.ex. digital ovana, språkbarriärer, flerstegsprocesser för familjer) och hur de hanteras? [2]

Referenser

Publicerade studier där de refererade funktionerna använts i skarp drift:

1. Gustafson Hedov E, Nyberg F, Gustafsson S, Li H, Gisslén M, Sundström J. Person-centered web-based mobile health system (Symptoms) for reporting symptoms in COVID-19 vaccinated individuals: observational study of system, users, and symptoms. JMIR Form Res. 2024;8:e57514. (Symptoms; RECOVAC/SCIFI-PEARL)
2. Ekholm K, Augustinsson A, Sundström J, m.fl. Implementing electronic informed consent in rare disease genomics. Sci Rep. 2025;15:44419. (MinForskning; GMS-RD)
3. Sundström J, Kristofi R, Östlund O, m.fl. A registry-based randomised trial comparing an SGLT2 inhibitor and metformin as standard treatment of early stage type 2 diabetes (SMARTTEST): rationale, design and protocol. J Diabetes Complications. 2021;35:107996. (MinForskning; SMARTTEST)
4. af Geijerstam P, Johansson E, Fägerstam S, m.fl. Effect of the FoodSwitch application on type 2 diabetes in Sweden: a study protocol for the randomised controlled DIATEST-HELP trial. BMJ Open. 2025;15:e110141. (MinForskning och Symptoms; DIATEST-HELP)
5. Integritetsskyddsmyndigheten. Förhandssamråd enligt dataskyddsförordningen, dnr IMY-2026-8907, 2026-06-24.

Checklistan är ett stöd för kravställning och gör inte anspråk på att vara uttömmande. Den är leverantörsneutral: samtliga frågor kan ställas till valfri leverantör och besvaras med ja, nej, eller på vilket sätt.

Bilaga. Regelverkskoppling per avsnitt

Kopplingen anges per avsnitt (tema) snarare än rad för rad, för att bilagan ska vara överblickbar. Den är vägledande, inte en fullständig juridisk analys.

Avsnitt	Huvudsaklig regelverkskoppling
1. Laglig grund, dataskydd och informationssäkerhet	GDPR art. 5, 6, 9, 24, 28, 32–34 (behandlingsprinciper, laglig grund, känsliga uppgifter, säkerhet, PUB-avtal, incidentrapportering); institutionens informationsklassning (t.ex. KRT 3:3:1); arkivlagstiftning
2. Identifikation och signering	GDPR art. 5.1 d (riktighet), art. 32 (säkerhet); eIDAS-förordningen; EU CTR 536/2014 art. 29 (samtycke och vårdnadshavare vid kliniska prövningar)
3. Regulatoriska frågor och spårbarhet	EU CTR 536/2014; ICH E6 (GCP); FDA 21 CFR Part 11; EudraLex Annex 11; GDPR art. 5.2 (ansvarsskyldighet/audit trail)
4. Deltagarens rättigheter över tid	GDPR art. 7 (samtyckets villkor och återkallelse), art. 12–15 (information och rättigheter); EU CTR 536/2014 art. 29.3 (återkallelse)
5. Inkludering och tillgänglighet	Lagen om tillgänglighet till digital offentlig service (DOS-lagen, 2018:1937) och WCAG 2.1; GDPR art. 12 (klart och tydligt språk); lagen om etikprövning av forskning som avser människor (2003:460)
6. Stark autentisering av deltagaren	GDPR art. 32 (säkerhet), art. 9 (känsliga personuppgifter); institutionens informationsklassning; IMY:s yttrande dnr IMY-2026-8907, råd 4
7. Riktighet, identitetsbindning och registerlänkning	GDPR art. 5.1 d (riktighet); IMY:s yttrande råd 4–5; relevant registerförfattning vid länkning (t.ex. patientdatalagen, biobankslagen)
8. Instrument, datakvalitet och datatyper	GDPR art. 5.1 c och d (uppgiftsminimering och riktighet) — i huvudsak metodologiska/vetenskapliga krav snarare än regulatoriska
9. Longitudinell insamling och följsamhet	GDPR art. 5.1 e (lagringsminimering); lagen om etikprövning (uppföljning inom godkänt ändamål)
10. Kommunikation och återkoppling	GDPR art. 32 (säkerhet vid kommunikation), art. 9 (känsliga uppgifter); patientdatalagen vid återkoppling av kliniska fynd
11. Integration, interoperabilitet och export	GDPR art. 5.1 f och art. 25 (integritet, konfidentialitet, inbyggt dataskydd); art. 32 och art. 35.7 d (pseudonymisering); IMY:s yttrande råd 6
12. Drift, kontinuitet och avtalsfrågor	GDPR art. 28 (biträdesavtal), art. 32 (kontinuitet och återställande); relevant upphandlingslagstiftning (LOU) avseende exit och immateriella rättigheter
13. Uppföljning, granskning och dokumenterad erfarenhet	GDPR art. 35.11 (regelbunden översyn); IMY:s yttrande råd 1 och 3; lagen om etikprövning (dokumenterad erfarenhet)