Europeiska kommissionen

TILLSTÅNDET I UNIONEN 2018

Skydda EU-medborgarnas personuppgifter i val

#SOTEU

12 september 2018

”Jag vill att EU-medborgarna ska kunna gå till valurnorna i maj nästa år i ett rättvist, säkert och öppet Europaparlamentsval. I dagens uppkopplade värld är risken för inblandning och manipulering högre än någonsin. Det är dags att vi anpassar våra regler till den digitala tidsåldern för att skydda den europeiska demokratin.”

Jean-Claude Juncker, 12 september 2018

Politiska partier använder i allt oftare personuppgifter för att nå medborgarna på olika sociala medier under valkampanjer. Avslöjandena om Cambridge Analytica visar vilka risker den moderna tekniken kan utsätta valprocessen för. Kommissionen har i dag fastställt riktlinjer för hur befintliga EU-regler ska användas för att ta itu med detta problem och säkerställa en rättvis valprocess, i synnerhet inför valet till Europaparlamentet 2019.

EU:s allmänna dataskyddsförordning trädde i kraft i maj 2018. Den innehåller tydliga regler om hur alla aktörer som är inblandade i val måste fullgöra sina funktioner och följa de nya dataskyddsreglerna.

Vilka skyldigheter har politiska partier och stiftelser

Politiska partier och stiftelser är personuppgiftsansvariga, eftersom de bestämmer varför och hur personuppgifter behandlas.

GÖR SÅ HÄR:

- Välj **den rätta rättsliga grunden** för personuppgiftsbehandling och var uppmärksam på de särskilda villkoren för behandling av känsliga data.
- Försäkra dig om att de system du använder är **säkra** och rapportera omedelbart eventuella dataläckor.
- Underrätta berörda individer när du börjar behandla deras data – även när dessa har samlats in från en tredje part.
- Säkerställ att de data som du behandlar är korrekta, särskilt om de har sammanställts från olika källor.
- Om du använder tjänster från en **tredje part** – exempelvis ett dataanalysföretag – ska du kontrollera att de data som kommer från denna part har erhållits på lagligt sätt.

GÖR INTE SÅ HÄR:

- Behandla inte personuppgifter som har uppgetts i ett **syfte** som inte har med valet att göra.
- Bevilja inte omfattande **åtkomsträttigheter** till personuppgifter som du har tillgång till. Kontrollera vilka i din organisation som har åtkomst till uppgifterna och för vilka legitima ändamål.

Dataanalysföretag och datamäklare

Dataanalysföretag och datamäklare är antingen personuppgiftsansvariga eller personuppgiftsbiträden beroende på hur stor kontroll de har över databehandlingen. Exempel: Om ett dataanalysföretag behandlar personuppgifter enligt instruktioner från ett politiskt parti så är det är det ett personuppgiftsbiträde.

GÖR SÅ HÄR:

- Välj **lämplig rättslig grund** för personuppgiftsbehandlingen

  Nedanstående text gäller endast om dataanalysföretaget eller datamäklaren är personuppgiftsansvarig

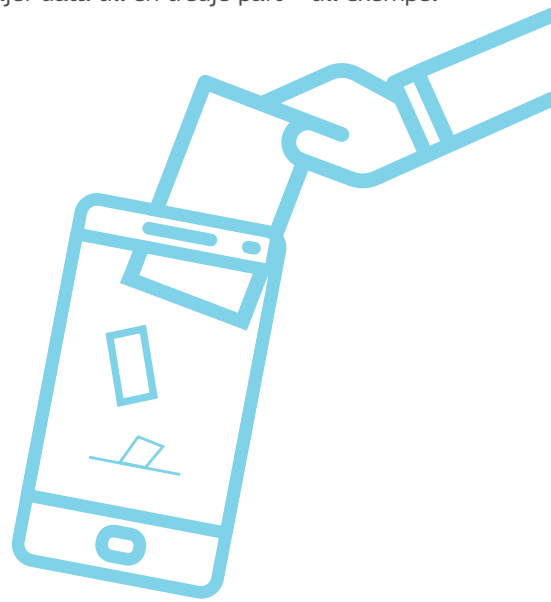
- Om du behandlar **känsliga data** (t.ex. etniskt ursprung) behöver du den berörda personens uttryckliga samtycke, eller tillämpa undantag som föreskrivs i den allmänna dataskyddsförordningen.
- Försäkra dig om att de system du använder är **säkra** och rapportera omedelbart eventuella dataläckor.
- Om du kombinerar olika **datauppsättningar** ska du se till att det sker på ett noggrant och lagligt vis.

  Den sista punkten gäller endast om dataanalysföretaget eller datamäklaren är personuppgiftsbiträde.

- Hjälp **tredje parter** som du samarbetar med – som politiska partier – om de behöver din hjälp, till exempel med att utarbeta en konsekvensbedömning avseende dataskydd.

GÖR INTE SÅ HÄR:

- Behandla inte personuppgifter som har uppgetts i ett **syfte** som inte har med valet att göra.
- Underrätta berörda personer varje gång data behandlas, särskilt om du säljer data till en tredje part – till exempel ett politiskt parti.



Nationella valmyndigheter

De nationella valmyndigheterna är **personuppgiftsansvariga**, eftersom de har kontroll över röstlängden.

GÖR SÅ HÄR:

Genomför en **konsekvensbedömning** avseende dataskydd för att bedöma riskerna innan du börjar behandla personuppgifter.

Den **rättsliga grunden** för personuppgiftsbehandling handlar vanligtvis om att uppfylla en rättslig skyldighet eller utföra en lagbaserad uppgift av allmänintresse.

Plattformar för sociala medier

Plattformar för sociala medier är personuppgiftsansvariga, eftersom behandlingen av personuppgifter sker på deras plattformar.

GÖR SÅ HÄR:

- Välj **lämplig rättslig grund** för personuppgiftsbehandlingen
- Om du behandlar **känsliga data** (t.ex. etniskt ursprung) behöver du den berörda personens uttryckliga samtycke, eller tillämpa undantag som föreskrivs i den allmänna dataskyddsförordningen.
- Ge människor tillgång till **kontrollfunktioner och inställningar** så att de kan utöva sina rättigheter i praktiken, till exempel när de begär korrigering eller borttagning av sina uppgifter.
- Försäkra dig om att de system du använder är **säkra** och rapportera omedelbart eventuella dataläckor.

GÖR INTE SÅ HÄR:

- Utbyt inte data med **tredje parter**, exempelvis dataanalysföretag, såvida inte användaren har gett sitt uttryckliga samtycke.
- Om du delar användarnas data med tredje parter ska detta tydligt anges i villkoren för plattformen.

Print ISBN 978-92-79-92226-8 doi:10.2775/79933 NA-01-18-839-SV-C
PDF ISBN 978-92-79-92223-7 doi:10.2775/220320 NA-01-18-839-SV-N