EUROPA-
KOMMISSIONEN

Bruxelles, den 12.9.2018
COM(2018) 638 final

Frie og retfærdige valg

VEJLEDENDE DOKUMENT

Kommissionens vejledning i anvendelsen af Unionens databeskyttelseslovgivning i forbindelse med afholdelse af valg

Et bidrag fra Europa-Kommissionen til mødet mellem lederne i Salzburg den 19.-20. september 2018

KOMMISSIONENS VEJLEDNING I ANVENDELSEN AF UNIONENS DATABESKYTTELSESLOVGIVNING I FORBINDELSE MED AFHOLDELSE AF VALG

Dialog med vælgerne udgør grundlaget for den demokratiske proces. Det er fast praksis for politiske partier at tilpasse valgkommunikation til publikum under hensyntagen til deres særlige interesser. Det er derfor naturligt for aktører, der er involveret i valg, at udforske mulighederne for at anvende data med henblik på at vinde stemmer. Den stadig mere udbredte anvendelse af digitale værktøjer og onlineplatforme har skabt mange nye muligheder for at nå ud til folk i den politiske debat.

Den stigende mikromålretning af kommunikation mod vælgere på grundlag af ulovlig behandling af personoplysninger, sådan som det blev konstateret i forbindelse med afsløringen af Cambridge Analytica, er imidlertid af en anden art. Den illustrerer de udfordringer, som moderne teknologi indebærer, men det dokumenterer også, at databeskyttelse er særlig vigtig i forbindelse med valg. Spørgsmålet er blevet et centralt emne, ikke kun for enkeltpersoner, men også for den måde, vores demokratier fungerer på, fordi det udgør en alvorlig trussel mod en retfærdig og demokratisk valgproces og har potentiale til at undergrave en åben debat, retfærdighed og gennemsigtighed, hvilket er afgørende i et demokrati. Kommissionen finder det yderst vigtigt at behandle dette spørgsmål for at genoprette offentlighedens tillid til, at valgprocesser er retfærdige.

De første rapporter fra Det Forenede Kongeriges databeskyttelsesmyndighed (Information Commissioner's Office – ICO) om anvendelsen af dataanalyse i politiske kampagner[1] og udtalelsen fra Den Europæiske Tilsynsførende for Databeskyttelse om onlinemanipulation og personoplysninger[2] har bekræftet den stigende betydning i valgsammenhæng af mikromålretning, som oprindeligt blev udviklet til kommercielle formål.

Mere generelt har flere databeskyttelsesmyndigheder behandlet spørgsmålet om databeskyttelse i forbindelse med valg[3].

Europa-Parlamentets og Rådets forordning (EU) 2016/679 (generel forordning om databeskyttelse)[4], der fra den 25. maj 2018 blev umiddelbart gældende i hele Unionen, giver Unionen de nødvendige redskaber til at imødegå tilfælde af ulovlig anvendelse af personoplysninger i forbindelse med

[1] Rapporter fra Det Forenede Kongeriges databeskyttelsesmyndighed (Information Commissioner's Office – ICO) af 10. juli 2018: "Investigation into the use of data analytics in political campaigns — Investigation update" and " Democracy Disrupted? Personal information and political influence".

[2] https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf.

[3] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3013267 "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" offentliggjort af Italiens databeskyttelsesmyndighed i den italienske statstidende nr. 71 den 26.3.2014 [doc. web n. 3013267]; https://www.cnil.fr/fr/communication-politique-quelles-sont-les-regles-pour-lutilisation-des-donnees-issues-des-reseaux "Communication politique: quelles sont les règles pour l'utilisation des données issues des réseaux sociaux?" offentliggjort af Commission Nationale de l'informatique et des libertés (Frankrigs nationale kommission for informatik og frihed) 8.11.2016; https://ico.org.uk/media/for-organisations/documents/1589/promotion_of_a_political_party.pdf Information Commissioner's Office "Guidance on political campaigning" [20170426].

[4] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

afholdelse af valg. Der kræves imidlertid en fast og konsekvent anvendelse af reglerne, hvis de skal bidrage til at beskytte de demokratiske politikkers integritet. Da disse regler for første gang vil blive anvendt ved et valg på EU-plan i forbindelse med det kommende valg til Europa-Parlamentet, er det vigtigt at tydeliggøre reglerne over for de aktører, som medvirker i valgprocessen — såsom nationale valgmyndigheder, politiske partier, datamæglere og dataanalytikere, sociale medieplatforme og onlinereklame-netværk. Denne vejledning har til formål at fremhæve databeskyttelsesforpligtelserne af relevans for valg. De nationale databeskyttelsesmyndigheder skal som håndhævere af den generelle forordning om databeskyttelse gøre fuld brug af deres styrkede beføjelser til at imødegå eventuelle overtrædelser, navnlig dem, der vedrører mikromålretning mod vælgerne.

1. EU's databeskyttelsesramme

Beskyttelsen af personoplysninger er en grundlæggende rettighed, der er forankret i Den Europæiske Unions charter om grundlæggende rettigheder (artikel 8) og i traktaterne (artikel 16 i TEUF). Den generelle forordning om databeskyttelse styrker rammerne for databeskyttelse og gør Unionen bedre rustet til at håndtere tilfælde af misbrug af personoplysninger i fremtiden, og alle aktører gøres mere ansvarlige for, hvordan de behandler personoplysninger.

Den giver enkeltpersoner i Unionen yderligere og stærkere rettigheder, som er særlig relevante i forbindelse med valg. Den databeskyttelsesordning, der var gældende i Unionen i de foregående 20 år, led især under den fragmenterede anvendelse af reglerne mellem medlemsstaterne, manglen på formaliserede samarbejdsmekanismer mellem de nationale databeskyttelsesmyndigheder og disse myndigheders begrænsede håndhævelsesbeføjelser. I den generelle forordning om databeskyttelse tages der højde for disse mangler: med udgangspunkt i de afprøvede databeskyttelsesprincipper harmoniseres centrale begreber med forordningen, såsom samtykke, enkeltpersoners ret til at få oplysninger om, hvordan deres data behandles, styrkes, det afklares, på hvilke betingelser personoplysninger kan videreformidles, der indføres regler for brud på personoplysningers sikkerhed, der etableres en samarbejdsmekanisme mellem datatilsynsmyndigheder i sager, som går på tværs af landegrænser, og deres håndhævelsesbeføjelser styrkes. Overtrædes EU's databeskyttelsesregler, har databeskyttelsesmyndighederne beføjelser til at undersøge (f.eks. ved at give påbud om at forelægge oplysninger og foretage inspektioner hos dataansvarlige og databehandlere) og rette op på adfærden (f.eks. ved at udstede advarsler og irettesættelser eller pålægge en midlertidig eller definitiv suspension af behandlingen). De har også beføjelse til at pålægge bøder på op til 20 mio. EUR eller, hvis der er tale om en virksomhed, op til 4 % af dens samlede omsætning på verdensplan[5]. Når de træffer afgørelse om at pålægge bøder og om bødeniveauet, skal databeskyttelsesmyndighederne tage hensyn til den enkelte sags omstændigheder og faktorer såsom behandlingens art, omfang eller formål, antallet af berørte

[5] Kommissionens vejledning om den generelle forordning om databeskyttelse findes på: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_da.

personer og omfanget af den skade, de har lidt[6]. I forbindelse med valg er det sandsynligt, at overtrædelsens grovhed og antallet af berørte personer vil være højt. Dette kan føre til, at der pålægges høje bøder, navnlig i betragtning af hvor væsentligt dette spørgsmål er for borgernes tillid til den demokratiske proces.

Det nyligt oprettede Europæiske Databeskyttelsesråd, som samler alle nationale databeskyttelsesmyndigheder og Den Europæiske Tilsynsførende for Databeskyttelse, spiller en central rolle i anvendelsen af den generelle forordning om databeskyttelse ved at udstede retningslinjer, anbefalinger og bedste praksis[7]. De nationale databeskyttelsesmyndigheder har som håndhævere af den generelle forordning om databeskyttelse og interessenternes direkte kontaktpunkt gode forudsætninger for at skabe yderligere retssikkerhed vedrørende fortolkningen heraf. Kommissionen støtter aktivt dette arbejde.

Direktivet om databeskyttelse inden for elektronisk kommunikation, også kaldet e-databeskyttelsesdirektivet (Europa-Parlamentets og Rådets direktiv 2002/58/EF[8]), fuldender EU's databeskyttelsesramme og er relevant i forbindelse med valg, da direktivets anvendelsesområde omfatter regler for elektronisk fremsendelse af uanmodet kommunikation, herunder med henblik på direkte markedsføring. I e-databeskyttelsesdirektivet fastsættes også regler for lagring af oplysninger og adgang til allerede lagrede oplysninger, f.eks. cookies, der kan bruges til at spore brugerens onlineadfærd, i terminaludstyr som f.eks. en smartphone eller en computer. Kommissionens forslag til en forordning om databeskyttelse inden for elektronisk kommunikation ("e-databeskyttelsesforordningen")[9], som i øjeblikket foreligger til forhandling, bygger på de samme principper som e-databeskyttelsesdirektivet. Med den nye forordning udvides anvendelsesområdet ud over traditionelle teleoperatører til at omfatte internetbaserede elektroniske kommunikationstjenester.

2. De forskellige aktørers vigtigste forpligtelser

Den generelle forordning om databeskyttelse finder anvendelse på alle aktører, der er aktive i forbindelse med afholdelse af valg, såsom europæiske og nationale politiske partier (i det følgende benævnt "politiske partier"), europæiske og nationale politiske fonde (i det følgende benævnt "fonde"), platforme, dataanalysevirksomheder og offentlige myndigheder med ansvar for valgprocessen. De må udelukkende behandle personoplysninger (f.eks. navne og adresser) på en lovlig, rimelig og gennemsigtig måde til specifikke formål. De må ikke derudover anvende oplysningerne på en måde, der er uforenelig med de formål, hvortil de oprindeligt blev indsamlet. Behandling i journalistisk øjemed falder også ind under den generelle databeskyttelsesforordnings anvendelsesområde, men da retten til ytrings- og

[6] Artikel 83 i den generelle forordning om databeskyttelse.
[7] Den Europæiske Tilsynsførende for Databeskyttelse afgiver også udtalelser.
[8] Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (EFT L 201 af 31.7.2002, s. 37).
[9] Forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation) (COM(2017) 10 final).

informationsfrihed er vigtig i et demokratisk samfund[10], kan visse undtagelser og fravigelser gøre sig gældende i overensstemmelse med national ret.

Begrebet personoplysninger spænder vidt. Personoplysninger er alle data om en identificeret eller identificerbar fysisk person. De oplysninger, der behandles i forbindelse med valg, vil ofte omfatte særlige kategorier af personoplysninger ("følsomme oplysninger"), såsom politiske holdninger, fagforeningsmæssigt tilhørsforhold, etnisk oprindelse, seksuelle forhold osv., som er omfattet af en ordning[11] med mere udstrakt beskyttelse. Med dataanalyser kan der desuden udledes "følsomme oplysninger" (f.eks. politiske holdninger, men også religiøse overbevisninger eller seksuel orientering) af sæt af ikkefølsomme oplysninger. Behandlingen af sådanne udledte oplysninger falder også ind under den generelle databeskyttelsesforordnings anvendelsesområde, og de bør derfor være i overensstemmelse med alle databeskyttelsesregler.

Det konkluderes, at praktisk taget alle databehandlingsoperationer i forbindelse med valg er omfattet af den generelle forordning om databeskyttelse.

I lyset af behovet for at tydeliggøre reglerne over for de aktører, som medvirker i valgprocessen, og af de første undersøgelsesresultater i Cambridge Analytica-sagen beskrives i de følgende afsnit de databeskyttelsesforpligtelser, der forekommer særlig relevante i forbindelse med valg. De sammenfattes i bilaget.

2.1 Dataansvarlige og databehandlere

Begrebet ansvarlighed for dataansvarlige og fælles dataansvarlige er et centralt element i den generelle forordning om databeskyttelse. Den dataansvarlige er den organisation, der afgør, alene eller i samarbejde med andre, hvorfor og hvordan personoplysningerne behandles; databehandleren behandler udelukkende personoplysninger på vegne af og efter instruks fra den dataansvarlige (idet deres indbyrdes forhold fastsættes i en kontrakt eller et andet juridisk bindende dokument). De dataansvarlige skal indføre foranstaltninger, der er passende i forhold til risiciene, og gennemføre indbygget databeskyttelse fra første færd, og de skal kunne godtgøre efterlevelsen af den generelle forordning om databeskyttelse (princippet om ansvarlighed).

Rollen som dataansvarlig og databehandler skal vurderes i hvert enkelt tilfælde. I forbindelse med valg kan en række aktører være dataansvarlige: politiske partier, individuelle kandidater og fonde er i de fleste tilfælde dataansvarlige; platforme og dataanalysevirksomheder kan være (fælles) dataansvarlige eller databehandlere for en nærmere bestemt behandling afhængigt af omfanget af den kontrol, de har med den pågældende behandling[12]; nationale valgmyndigheder er dataansvarlige for valglister.

[10] Artikel 85, stk. 2, i den generelle forordning om databeskyttelse.
[11] Artikel 9, stk. 1, i den generelle forordning om databeskyttelse.
[12] Ifølge nyere retspraksis fra Den Europæiske Unions Domstol (Jehovas Vidner-sagen C-25/17, dom af 10. juli 2018) blev det præciseret, at en organisation, der "udøver indflydelse på" indsamling og behandling af personoplysninger, under visse omstændigheder kan betragtes som dataansvarlig.

Når behandlingen vedrører udbud af varer og tjenesteydelser til enkeltpersoner i Unionen eller overvågning af deres adfærd i Unionen, skal virksomheder, der er etableret uden for Unionen, også overholde den generelle forordning om databeskyttelse. Dette er tilfældet for en række platforme og dataanalysevirksomheder.

2.2 Principper, lovlig behandling af og særlige betingelser for "følsomme oplysninger"

Aktører, der medvirker i valg, må kun behandle personoplysninger, herunder oplysninger fra offentlige kilder, efter principperne for behandling af personoplysninger og på grundlag af et antal begrænsede forudsætninger, som er klart angivet i den generelle forordning om databeskyttelse[13]. De mest relevante forhold, der skal gøre sig gældende for, at der er tale om lovlig behandling i forbindelse med valg, forekommer at være en enkeltpersons samtykke, overholdelse af en retlig forpligtelse i henhold til EU-retten eller national lovgivning, udførelse af en opgave af i samfundets interesse og en af aktørernes legitime interesse. Dog kan aktører i forbindelse med valg alene påberåbe sig at have en legitim interesse, hvis deres interesser ikke må vige for de berørte enkeltpersoners interesser eller grundlæggende rettigheder og frihedsrettigheder.

Lagring af oplysninger eller adgang til oplysninger, der allerede er lagret i terminaludstyr (computer, smartphone osv.), skal desuden ske i overensstemmelse med e-databeskyttelsesdirektivets krav om beskyttelse af terminaludstyr, hvilket indebærer, at den pågældende enkeltperson vil skulle give sit samtykke.

Når samtykke anvendes som retsgrundlag, kræves det i henhold til den generelle forordning om databeskyttelse, at dette gives gennem en klar og positiv bekræftelse, og at det foregår på et frivilligt og velinformeret grundlag[14].

Offentlige myndigheder, der medvirker i valgprocessen, behandler personoplysninger for at overholde en retlig forpligtelse eller udføre en offentlig opgave. Andre aktører kan i forbindelse med valg behandle data på grundlag af samtykke eller legitim interesse[15]. Politiske partier og fonde kan også behandle data på grundlag af samfundsinteresser, hvis dette er foreskrevet i den nationale ret[16].

Offentlige myndigheder må kun videregive visse oplysninger om enkeltpersoner, der er opført på valglister eller i adresseregistre over bosiddende personer, til politiske partier, når dette specifikt er tilladt i henhold til medlemsstaternes nationale ret og kun i forbindelse med reklame i forbindelse med valg og i det omfang, det er nødvendigt til formålet, som f.eks. navn og adresse.

---

[13] Artikel 5 og 6 i den generelle forordning om databeskyttelse.
[14] Artikel 7, og artikel 4, nr. 11), i den generelle forordning om databeskyttelse.
[15] Dog forudsat, at de pågældende enkeltpersoners rettigheder og frihedsrettigheder ikke påvirkes i alvorlig grad.
[16] Jf. 56. betragtning i den generelle forordning om databeskyttelse: "hvis det i forbindelse med afholdelse af valg i en medlemsstat er nødvendigt, for at det demokratiske system kan fungere, at politiske partier indsamler personoplysninger om enkeltpersoners politiske holdninger, kan behandling af sådanne oplysninger tillades af hensyn til varetagelsen af samfundsinteresser, såfremt fornødne garantier er etableret".

Behandling af oplysninger i forbindelse med valg vil ofte omfatte "følsomme oplysninger". Behandling af sådanne oplysninger, herunder udledte "følsomme oplysninger", er generelt forbudt, medmindre et af de særlige forhold i den generelle forordning om databeskyttelse[17] gør sig gældende. Behandling af "følsomme oplysninger" forudsætter, at specifikke, strengere betingelser opfyldes: personen skal have givet udtrykkeligt samtykke[18] eller have offentliggjort oplysningerne[19]. Politiske partier og fonde må også behandle "følsomme oplysninger", hvis der er tale om væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret, og der er indført passende sikkerhedsforanstaltninger[20]. Ifølge den generelle forordning om databeskyttelse må de ligeledes behandle "følsomme oplysninger", for så vidt som de udelukkende vedrører egne medlemmer eller tidligere medlemmer, eller personer der har regelmæssig kontakt med dem – men kun til videregivelse inden for deres politiske parti eller fond[21]. Et politisk parti må dog ikke benytte denne specifikke bestemmelse med henblik på at behandle oplysninger om potentielle medlemmer eller vælgere.

Formålet med databehandlingen bør præciseres på indsamlingstidspunktet (princippet om "formålsbegrænsning")[22]. Data, der indsamles til et givet formål, må alene viderebehandles til formål, der er forenelige hermed; i modsat fald skal der findes et nyt retsgrundlag i henhold til den generelle forordning om databeskyttelse, f.eks. samtykke, for at behandlingen kan foretages til det nye formål. Navnlig må data ikke viderebehandles i forbindelse med valg, hvis dataene omhandler livsstil og er indsamlet af datamæglere eller platforme til kommercielle formål.

Medmindre politiske partier og fonde udviser behørig omhu og kontrollerer, at oplysningerne er tilvejebragt på lovlig vis, må de ikke anvende sådanne data modtaget fra tredjemand.

2.3 Gennemsigtighedskrav

Cambridge Analytica-sagen har vist, hvor vigtigt det er at bekæmpe uigennemskuelighed og informere de berørte enkeltpersoner korrekt. Enkeltpersoner ved ofte ikke, hvem der behandler deres personoplysninger, og til hvilket formål. Principperne om rimelig og gennemsigtig behandling forudsætter, at enkeltpersoner oplyses om behandlingsaktiviteters eksistens og deres formål[23]. I den generelle forordning om databeskyttelse præciseres de dataansvarliges forpligtelser i den henseende. De skal oplyse enkeltpersoner om de vigtigste aspekter i forbindelse med behandlingen af deres personoplysninger, f.eks.:

- den dataansvarliges identitet
- formålene med behandlingen

[17] Artikel 9 i den generelle forordning om databeskyttelse.
[18] Artikel 9, stk. 2, litra a), i den generelle forordning om databeskyttelse.
[19] Artikel 9, stk. 2, litra e), i den generelle forordning om databeskyttelse.
[20] Artikel 9, stk. 2, litra g), i den generelle forordning om databeskyttelse.
[21] Artikel 9, stk. 2, litra d), i den generelle forordning om databeskyttelse. Politiske partier eller fonde må ikke dele oplysninger vedrørende egne medlemmer eller tidligere medlemmer, eller enkeltpersoner der har regelmæssig kontakt med dem, med tredjemand uden de berørte enkeltpersoners samtykke.
[22] Artikel 5, stk. 1, litra b), i den generelle forordning om databeskyttelse.
[23] Artikel 5, stk. 1, litra a), i den generelle forordning om databeskyttelse.

- hvem der modtager personoplysningerne
- kilden til dataene, når disse ikke er indsamlet direkte fra personen
- forekomsten af automatiske afgørelser og
- eventuelle yderligere oplysninger, der er nødvendige for at sikre en rimelig og gennemsigtig behandling[24].

Ifølge den generelle forordning om databeskyttelse skal oplysningerne endvidere gives i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog[25]. For eksempel vil en kort, uigennemskuelig meddelelse om databeskyttelse, der alene trykkes i en lille skriftstørrelse i valgmaterialer, ikke opfylde kravene om gennemsigtighed.

Ifølge de foreløbige undersøgelsesresultater var ufuldstændige oplysninger om formålet med indsamlingen af oplysninger en central mangel i Cambridge Analytica-sagen, og dette rejste også tvivl om gyldigheden af de berørte personers samtykke. Alle organisationer, der behandler personoplysninger i forbindelse med valg, skal sikre sig, at enkeltpersoner fuldt ud forstår, hvordan og til hvilket formål deres personoplysninger vil blive brugt, inden de giver deres samtykke, eller inden den dataansvarliges behandling påbegyndes med en anden hjemmel for behandlingen som grundlag.

Der skal gives oplysninger til enkeltpersoner på hvert trin i behandlingen og ikke kun, når dataene indsamles.

Når politiske partier behandler oplysninger fra tredjemand (f.eks. fra valglister, datamæglere, dataanalytikere og andre kilder), skal de almindeligvis underrette og forklare de pågældende enkeltpersoner, hvordan de kombinerer og anvender disse oplysninger, således at en rimelig behandling sikres[26].

2.4 Profilering, automatiske afgørelser og mikromålretning

Profilering er en form for automatisk behandling af personoplysninger, der anvendes til at analysere eller forudsige forhold vedrørende personlige præferencer, interesser, økonomiske forhold osv.[27]. Profilering kan bruges til mikromålretning mod enkeltpersoner ved at analysere personoplysninger (f.eks. en søgehistorie på internettet) for at afdække en bestemt gruppes eller persons særlige interesser med henblik på at påvirke den pågældende gruppes eller persons handlinger. Mikromålretning kan benyttes til at sende en personlig besked til en enkeltperson eller et publikum ved hjælp af en onlinetjeneste, f.eks. sociale medier.

Cambridge Analytica-sagen har vist de særlige udfordringer, der opstår som følge af mikromålretningsmetoder på de sociale medier. Organisationerne kan benytte de data, der er indsamlet gennem brugerne af de sociale medier, til at skabe vælgerprofiler. Det kan give sådanne organisationer mulighed for at udpege vælgere, der lettere kan påvirkes, og dermed gøre det muligt for sådanne organisationer at øve indflydelse på valgresultatet.

[24] Artikel 13 og 14 i den generelle forordning om databeskyttelse.
[25] Retningslinjer fra Det Europæiske Databeskyttelsesråd om gennemsigtighed.
[26] Artikel 14 i den generelle forordning om databeskyttelse.
[27] Jf. definitionen i artikel 4, nr. 4), i den generelle forordning om databeskyttelse.

Alle generelle principper og regler i den generelle forordning om databeskyttelse finder anvendelse på behandling af sådanne oplysninger, såsom princippet om lovlighed, rimelighed og gennemsigtighed. Enkeltpersoner er meget ofte ikke klar over, at de udsættes for profilering: de forstår ikke, hvorfor de modtager reklamer, der tydeligvis hænger sammen med deres seneste søgninger, eller hvorfor de modtager personaliserede beskeder fra forskellige organisationer. Ved den generelle forordning om databeskyttelse forpligtes alle dataansvarlige, f.eks. politiske partier eller dataanalytikere, til at oplyse de pågældende enkeltpersoner, når de anvender sådanne teknikker, og om forventede konsekvenser[28] heraf.

I den generelle forordning om databeskyttelse anerkendes det, at automatiske afgørelser, herunder profilering, kan have alvorlige konsekvenser. Ifølge den generelle forordning om databeskyttelse har en enkeltperson ret til ikke at være genstand for en afgørelse, som alene er baseret på automatisk behandling, og som har retsvirkning for vedkommende, eller som på tilsvarende vis betydeligt påvirker den pågældende, medmindre en sådan behandling foretages på strenge betingelser, dvs. hvis enkeltpersoner giver deres udtrykkelige samtykke, eller når det er tilladt ifølge EU-retten eller medlemsstaternes nationale ret, hvori der fastsættes tilstrækkelige beskyttelsesforanstaltninger[29].

Praksis, som benytter mikromålretning i forbindelse med valg, tilhører denne kategori, hvis den har en tilstrækkeligt væsentlig virkning på enkeltpersoner. Det Europæiske Databeskyttelsesråd har anført, at dette er tilfældet, hvis afgørelsen har potentiale til at påvirke enkeltpersoners omstændigheder, adfærd eller valg i væsentlig grad eller har en langvarig eller varig indvirkning på den enkelte[30]. Databeskyttelsesrådet fandt, at onlinemålrettede reklamer under visse omstændigheder kan påvirke enkeltpersoner i tilstrækkelig grad, hvis de eksempelvis er påtrængende eller anvender viden om enkeltpersoners svage punkter. I betragtning af, hvor vigtigt det er at kunne udøve den demokratiske stemmeret, kan personaliserede beskeder, der f.eks. kan betyde, at enkeltpersoner afholder sig fra at deltage i afstemningen eller stemmer på en bestemt måde, potentielt opfylde kriteriet om, at der er tale om en væsentlig påvirkning.

I forbindelse med valg er de dataansvarlige derfor nødt til at sikre, at enhver behandling, der foregår ved hjælp af sådanne teknikker, er lovlig ifølge ovennævnte principper og de strenge betingelser i den generelle forordning om databeskyttelse.

2.5 Sikkerhed og rigtighed i relation til personoplysninger

Sikkerhed er særlig vigtig i forbindelse med valg i betragtning af omfanget af de pågældende datasæt og det forhold, at sådanne sæt ofte indeholder "følsomme oplysninger". I henhold til den generelle forordning om databeskyttelse skal operatører, der behandler personoplysninger (både dataansvarlige og databehandlere), gennemføre passende tekniske og organisatoriske

[28] Artikel 13, stk. 2, i den generelle forordning om databeskyttelse.
[29] Artikel 22 i den generelle forordning om databeskyttelse.
[30] Retningslinjer fra Det Europæiske Databeskyttelsesråd om automatiske afgørelser, WP251rev.01, som senest ændret og vedtaget den 6.2.2018.

foranstaltninger for at sørge for et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer for enkeltpersoners rettigheder og frihedsrettigheder[31].

Ifølge den generelle forordning om databeskyttelse skal den dataansvarlige uden unødig forsinkelse og om muligt senest inden for 72 timer anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed. Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for enkeltpersoners rettigheder og frihedsrettigheder, underretter den dataansvarlige ligeledes uden unødig forsinkelse de enkeltpersoner, som berøres af bruddet på persondatasikkerheden[32].

Politiske partier og andre aktører, der medvirker i valgprocessen, skal være særlig opmærksomme på at sikre, at personoplysningerne er korrekte, når der er tale om omfangsrige datasæt, og når der indsamles data fra forskellige, heterogene kilder. Ukorrekte oplysninger skal straks slettes eller berigtiges og om nødvendigt ajourføres.

2.6 Konsekvensanalyse vedrørende databeskyttelse

Ved den generelle forordning om databeskyttelse indføres et nyt værktøj til vurdering af risikoen, inden behandlingen påbegyndes: konsekvensanalysen vedrørende databeskyttelse Dette er påkrævet, når behandlingen sandsynligvis vil medføre en høj risiko for de pågældende personers rettigheder og frihedsrettigheder[33]. Dette er tilfældet i forbindelse med valg, hvis en dataansvarlig foretager en systematisk og omfattende vurdering af personlige forhold vedrørende en enkeltperson (herunder profilering), der påvirker denne enkeltperson betydeligt, og hvis den dataansvarlige behandler "følsomme oplysninger" i stort omfang. De nationale valgmyndigheder, der udfører deres opgaver i samfundets interesse, behøver muligvis ikke at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis der allerede er foretaget en konsekvensanalyse vedrørende databeskyttelse i forbindelse med vedtagelsen af lovgivningen.

De konsekvensanalyser, der skal foretages af de forskellige aktører i forbindelse med valg, bør omfatte de elementer, der er nødvendige for at håndtere de risici, der er forbundet med en sådan behandling, navnlig hvorvidt behandlingen af datasæt fra tredjemand også er lovlig, tillige med gennemsigtighedskravene.

3. Enkeltpersoners rettigheder

I den generelle forordning om databeskyttelse gives enkeltpersoner i Unionen yderligere og stærkere rettigheder, som er særlig relevante i forbindelse med valg:

- ret til indsigt i deres personoplysninger

[31] Artikel 32 i den generelle forordning om databeskyttelse.
[32] Artikel 33 og 34 i den generelle forordning om databeskyttelse og retningslinjerne fra Det Europæiske Databeskyttelsesråd om anmeldelse af brud på persondatasikkerheden.
[33] Artikel 35 og 36 i den generelle forordning om databeskyttelse og retningslinjerne fra Det Europæiske Databeskyttelsesråd om konsekvensanalysen vedrørende databeskyttelse.

- ret til at anmode om at få slettet deres personoplysninger, hvis behandlingen er baseret på samtykke, og dette samtykke trækkes tilbage, hvis oplysningerne ikke længere er nødvendige, eller hvis behandlingen er ulovlig, og
- ret til at få rettet ukorrekte, unøjagtige eller ufuldstændige personoplysninger.

Enkeltpersoner har også ret til at gøre indsigelse mod behandling (f.eks. af oplysninger i valglister, der fremsendes til politiske partier), hvis behandlingen af deres oplysninger er begrundet i hensynet til "legitim interesse" eller "samfundets interesse".

Enkeltpersoner har ret til ikke at blive gjort til genstand for en afgørelse, som alene bygger på automatisk behandling af deres personoplysninger. Enkeltpersoner kan i sådanne tilfælde anmode om intervention fra en fysisk persons side og har ret til at fremkomme med deres synspunkter og til at bestride afgørelsen.

For at enkeltpersoner kan udøve disse rettigheder, skal alle involverede aktører stille de nødvendige værktøjer og indstillinger til rådighed. I den generelle forordning om databeskyttelse åbnes der mulighed for at udarbejde en adfærdskodeks, som er godkendt af en databeskyttelsesmyndighed, og som præciserer forordningens anvendelse på specifikke områder, herunder i forbindelse med valg.

I den generelle forordning om databeskyttelse indrømmes enkeltpersoner ret til at indgive klage til en tilsynsmyndighed og adgang til retsmidler. Enkeltpersoner gives også ret til at bemyndige en ikke-statslig organisation til at indgive en klage på deres vegne[34]. I nogle medlemsstater giver den nationale lovgivning mulighed for, at en ikke-statslig organisation kan indgive en klage uden at være bemyndiget af en enkeltperson. Dette er særlig relevant i forbindelse med valg på grund af det store antal potentielt berørte personer.

[34] Artikel 80, stk. 1, i den generelle forordning om databeskyttelse.

Centrale databeskyttelsesspørgsmål af relevans for valgprocessen[35]

Politiske partier og fonde	Politiske partier og fonde er dataansvarlige
	• Overhold formålsbegrænsning, viderebehandling alene til formål, der er forenelige (f.eks. når data deles med platforme) • Vælg det relevante retsgrundlag for behandlingen (også for udledte data): samtykke, legitim interesse, opgave i samfundets interesse (hvis fastsat ved lov), særlige betingelser, hvis det drejer sig om "følsomme oplysninger" (f.eks. politisk holdning) • Gennemfør en konsekvensanalyse vedrørende databeskyttelse • Informer enkeltpersoner om hvert enkelt behandlingsformål (krav om gennemsigtighed) enten i forbindelse med direkte indsamling af data eller ved indhentning af oplysninger fra tredjemand • Sørg for datanøjagtighed, navnlig for data fra forskellige kilder og for udledte data • Kontroller, om oplysninger, der er modtaget fra tredjemand, er tilvejebragt lovligt og til hvilke formål (f.eks.: om de berørte personer gav deres informerede samtykke til et givet formål) • Tag hensyn til de specifikke risici ved profilering og indfør passende beskyttelsesforanstaltninger • Overhold særlige betingelser, når der anvendes automatiske afgørelser (indhent eksempelvis udtrykkeligt samtykke og indfør passende beskyttelsesforanstaltninger) • Angiv tydeligt, hvem der har adgang til oplysningerne • Sørg for behandlingssikkerhed gennem tekniske og organisatoriske foranstaltninger; indberet brud på datasikkerheden • Præciser forpligtelser i kontrakter eller andre juridisk bindende dokumenter for databehandlere, f.eks. dataanalysevirksomheder • Slet oplysningerne, når de ikke længere er nødvendige til det oprindelige formål, som de er indsamlet til
Datamæglere og	Datamæglere og dataanalysevirksomheder er enten (fælles)

[35] Ovenstående oplysninger er på ingen måde udtømmende. De har til formål at fremhæve en række centrale forpligtelser knyttet til data ifølge den generelle forordning om databeskyttelse, som er relevante for valgprocessen. De svarer til et scenarie, hvor de politiske partier selv indsamler data (fra offentlige kilder, fra deres tilstedeværelse på de sociale medier, direkte fra vælgerne osv.) og benytter sig af datamæglere eller dataanalysevirksomheder med henblik på målretning over for vælgere gennem sociale medieplatforme. Platforme kan også være en kilde til data for ovennævnte aktører. Anden lovgivning kan også være relevant, f.eks. reglerne om fremsendelse af uanmodet kommunikation og beskyttelse af terminaludstyr i e-databeskyttelsesdirektivet.

<table>
<tr><td rowspan="3">dataanalysevirksomheder</td><td colspan="2">dataansvarlige eller databehandlere, afhængigt af omfanget af den kontrol, de har med behandlingen</td></tr>
<tr><td>Som dataansvarlig</td><td>Som databehandler</td></tr>
<tr><td>• Overhold formålsbegrænsning, viderebehandling alene til formål, der er forenelige (navnlig når data deles med tredjeparter)
• Vælg det relevante retsgrundlag for behandlingen: samtykke, legitim interesse; drejer det sig om "følsomme oplysninger", må de alene behandles, hvis der er givet udtrykkeligt samtykke, eller oplysningerne tydeligvis er offentliggjort
• Gennemfør en konsekvensanalyse vedrørende databeskyttelse
• Informer enkeltpersoner om hvert enkelt behandlingsformål (krav om gennemsigtighed) — navnlig når der ansøges om samtykke, eftersom oplysningerne normalt vil blive solgt til en tredjepart
• Overhold særlige betingelser, når der anvendes automatiske afgørelser (indhent eksempelvis udtrykkeligt samtykke og indfør passende beskyttelsesforanstaltninger)
• Vær særlig opmærksom på behandlingens lovlighed, og at oplysningerne er korrekte, når forskellige datasæt kombineres
• Sørg for behandlingssikkerhed gennem tekniske og organisatoriske foranstaltninger; indberet brud på datasikkerheden</td><td>• Opfyld forpligtelser i kontrakten eller et andet juridisk bindende dokument indgået med den dataansvarlige
• Sørg for behandlingssikkerhed gennem tekniske og organisatoriske foranstaltninger
• Støt den dataansvarlige i forbindelse med konsekvensanalyser vedrørende databeskyttelse eller i forbindelse med udøvelsen af de registreredes rettigheder eller ved straks at underrette den dataansvarlige, hvis de bliver bekendt med et brud på datasikkerheden</td></tr>
<tr><td></td><td colspan="2">Platforme er normalt dataansvarlige for den behandling, der finder sted på deres platforme, og eventuelt fælles dataansvarlige sammen med andre organisationer</td></tr>
<tr><td>Sociale medieplatforme/ onlinereklame-netværk</td><td colspan="2">• Vælg det relevante retsgrundlag for behandlingen: kontrakt med enkeltpersoner, samtykke, legitim interesse; drejer det sig om "følsomme oplysninger", må de alene behandles, hvis der er givet udtrykkeligt samtykke, eller oplysningerne tydeligvis er offentliggjort</td></tr>
</table>

	• Brug kun de oplysninger, der er nødvendige til det fastsatte formål • Gennemfør en konsekvensanalyse vedrørende databeskyttelse • Sørg for, at deling af medlemmers data med tredjemand sker på lovlig vis • Overhold krav om gennemsigtighed, navnlig med hensyn til vilkår og betingelser, hvis oplysninger efterfølgende udveksles med tredjemand osv. • Overhold særlige betingelser, når der anvendes automatiske afgørelser (indhent eksempelvis udtrykkeligt samtykke og indfør passende beskyttelsesforanstaltninger) • Sørg for behandlingssikkerhed gennem tekniske og organisatoriske foranstaltninger; indberet brud på datasikkerheden • Sørg for, at enkeltpersoner gives kontrol og indstillinger, således at de effektivt kan udøve deres rettigheder, herunder retten til ikke at blive gjort til genstand for en afgørelse, som alene er baseret på automatisk behandling, herunder profilering
	Nationale valgmyndigheder er dataansvarlige
Nationale valgmyndigheder	• Retsgrundlag for behandlingen: retlig forpligtelse eller opgave i samfundets interesse baseret på lovgivning • Gennemfør en konsekvensanalyse vedrørende databeskyttelse, hvis konsekvenserne ikke allerede er vurderet i lovgivningen