



Bruxelles, den 12.9.2018
COM(2018) 637 final

**MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET,
DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG
REGIONSUDVALGET**

Sikring af frie og retfærdige valg til Europa-Parlamentet

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

DA

DA

Sikring af frie og retfærdige valg til Europa-Parlamentet

Et afgørende øjeblik for Den Europæiske Unions fremtid

Kernen i Den Europæiske Union er dens forsvar af demokratiet og demokratiske værdier. Disse er bydende nødvendige for et samfund, hvor pluralisme og tolerance er fremherskende, og hvor borgere i Unionen kan stemme i forvisning om, at de ikke vildledes. Demokrati er sammen med retsstatsprincippet og grundlæggende rettigheder en del af, "hvem vi er", og kendetegner vores Union.

Valget til Europa-Parlamentet i maj 2019 vil blive holdt på en baggrund, som er meget forskellig fra alle hidtidige valg. Unionen og dens medlemsstater står over for store politiske udfordringer. Der er et indlysende behov for at skabe en mere robust Union, der kan agere med troværdighed og styrke på verdensscenen, hvor de globale stormagter, der ikke nødvendigvis deler alle vores interesser eller værdier, kæmpes om at få magten. En robust Union på grundlag af et effektivt retligt samarbejde, udveksling af oplysninger med henblik på at imødegå terrorisme og organiseret kriminalitet og et velfungerende indre marked forudsætter gensidig tillid mellem medlemsstaterne og til vore demokratiske systemer. På den enestående baggrund vil valget til Europa-Parlamentet i maj 2019 forme Den Europæiske Unions fremtid i de kommende år.

En del af sikkerhedsunionen går ud på at øge modstandsdygtigheden i Unionens demokratiske systemer: angreb på valginfrastrukturer og kampagneinformationssystemer er hybride trusler, som Unionen er nødt til at forholde sig til. Politisk motiverede masseinformationskampagner på nettet, også med oprindelse i tredjelande, med det specifikke formål at miskreditere og svække legitimiteten af valg, er blevet anerkendt som voksende trusler mod vores demokratier¹. Den Europæiske Union bør træffe alle foranstaltninger, der ligger inden for rammerne af dens beføjelser, for at forsvare sine demokratiske processer mod manipulation fra tredjelande eller private interesser. Valgkampperioder har vist sig at være perioder, der er særligt udsatte for målrettet desinformation. Disse angreb påvirker valgprocessens integritet og retfærdighed og borgernes tillid til de valgte repræsentanter, og dermed udfordrer de selve demokratiet.

Borgerne i Unionen bør kunne stemme med fuldt overblik over de politiske valg, de har. Dette indebærer øget bevågenhed over for trusler og større gennemsigtighed i vores politiske proces. Et åbent offentligt rum, der beskytter mod utilbørlig påvirkning, sikrer lige vilkår for politiske kampagner og valgprocesser, som borgerne kan have tillid til². Det er afgørende for vore demokratier, at der skabes plads til en dynamisk politisk kampagne, som giver vælgerne et klart og ufordrejet billede af idéer og programmer i de partier, som konkurrerer om deres

¹ Jf. Fælles meddelelse til Europa-Parlamentet, Det Europæiske Råd og Rådet, Øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler (JOIN(2018) 16 final) og Det Europæiske Råds konklusioner af 28. juni 2018, (<http://www.consilium.europa.eu/da/press/press-releases/2018/06/29/20180628-euco-conclusions-final/pdf>).

² Europarådets Venedigkommission giver vejledning om valg ([http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2002\)023rev-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2002)023rev-e)), herunder for mediemiljøet ([http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI\(2016\)006-e](http://www.venice.coe.int/webforms/documents/?pdf=CDL-PI(2016)006-e)).

stemmer. Derfor bør svig og andre bevidste forsøg på at manipulere valget bekæmpes aktivt, herunder med sanktioner.

Onlineaktiviteter, herunder under valgkampprocessen, udvikler sig hurtigt, og øget sikkerhed og lige vilkår i valgkampen har derfor afgørende betydning. Traditionelle ("offline") garantier, såsom gældende regler for politisk kommunikation i løbet af valgkampperioder, gennemsigtighed af og begrænsninger for valgkostninger, overholdelse af eventuelle krav om, at der på valgdagen ikke føres valgkamp, og ligebehandling af kandidater, bør også gælde online³. Gennemsigtighed med hensyn til og grænser for politisk reklame på TV og reklametavler og gennemsigtighed i forbindelse med politisk reklame bør finde tilsvarende anvendelse i onlineverdenen. Dette er ikke tilfældet nu, og den situation må afhjælpes inden næste valg til Europa-Parlamentet.

Nye udfordringer og den seneste udvikling

Onlinekommunikation har mindsket hindringerne og omkostningerne for politiske aktører til at gå i dialog med borgerne og frembyder betydelige muligheder, men den har ligeledes øget ondsindede aktørers muligheder for at søge at påvirke den demokratiske debat og valgprocesserne. Onlinemiljøet kan gøre det lettere for aktører at fremlægge oplysninger og samtidig skjule deres oprindelse eller formål, herunder ved ikke at vise, at kommunikation (som f.eks. et opslag på de sociale medier) er en betalt reklame snarere end faktisk rapportering, der præsenterer holdninger som journalistik og selektivt præsenterer rapportering for at få spændinger til at blusse op eller polarisere debatten. Ingen bør tage let på disse trusler. Den Europæiske Union og dens politiske systemer er ikke immune over for sådanne trusler.

Desuden kan integriteten af valg påvirkes alvorligt af "konventionelle" cyberhændelser, herunder cyberangreb rettet mod valgprocesser, valgkampagner, politiske partiers infrastruktur, kandidater eller offentlige myndigheders systemer samt ved misbrug af personoplysninger. De seneste afsløringer, herunder angående "Facebook/Cambridge Analytica"-sagen, er et eksempel. Personoplysninger menes at være blevet misbrugt og ulovligt videregivet til tredjemand til formål, som afviger meget væsentligt fra de oprindeligt tiltænkte. Dette har understreget de potentielle risici ved visse onlineaktiviteter, der bruges til at påvirke borgerne målrettet i det skjulte med politisk reklame og kommunikation, ulovligt at behandle og misbruge deres personoplysninger til at manipulere holdninger, sprede

³ Jf. Europarådets nylige publikation "Internet and electoral campaigns – Study on the use of internet in electoral campaigns", der er udarbejdet af Europarådets ekspertudvalg om mediepluralisme og gennemsigtighed med hensyn til medieejerskab (MSI-MED) (<https://www.coe.int/en/web/human-rights-rule-of-law/-/internet-and-electoral-campaigns-a-new-study-has-been-published>). I undersøgelsen undersøges følgerne af, at valgreklamer flyttes over på internettet, navnlig hvad angår valgkostninger og reklameteknikker, der bygger på mikromålretning mod vælgerne med personaliserede beskeder. Jf. ligeledes Europarådets henstilling CM/Rec(2016)5 om internetfriheden, som omhandler statslige myndigheders, platformes og formidlers ansvar for politiske partiers, kandidaters og andre enkeltpersoners politiske kampagner online.

desinformation eller blot undergrave sandheden, når det tjener politiske formål eller øger splittelse⁴.

Støtte til frie og retfærdige valg i Unionen

EU-institutionerne afholder ikke valg. Det er primært medlemsstaternes ansvar at træffe foranstaltninger i den sammenhæng. Medlemsstaterne er ansvarlige for at afholde valg og for at overvåge valgprocessen⁵. Ikke desto mindre er EU-dimensionen selvindlysende. Ved at opstille kandidater til valg til Europa-Parlamentet er nationale og regionale politiske partier hovedaktører i valgkampagnerne til Europa-Parlamentet. De europæiske politiske partier og deres tilknyttede fonde har en vigtig funktion i forbindelse med at tilrettelægge supplerende kampagner på europæisk plan, herunder for spidskandidaterne til posten som formand for Europa-Kommissionen.

Efter valgene til Europa-Parlamentet i 2014 påtog Kommissionen sig i sin rapport fra 2015 om valget⁶ at identificere muligheder for en yderligere styrkelse af den europæiske dimension og den demokratiske legitimitet af EU's beslutningsproces og yderligere at undersøge og tage fat på årsagerne til den vedvarende lave valgdeltagelse i nogle medlemsstater. I februar 2018 opfordrede Kommissionen til, at borgerne tidligt og løbende inddrages i debatter om europæiske spørgsmål, at de politiske partier indleder deres kampagner tidligere, end det hidtil har været tilfældet, i forbindelse med valget til Europa-Parlamentet, herunder kampagner for deres kandidater til posten som formand for Europa-Kommissionen, at forbindelserne mellem nationale og europæiske politiske partier gøres mere gennemsigtige, og at medlemsstaterne tilskynder vælgerne til at benytte deres stemmeret, navnlig for underrepræsenterede grupper.

Den Europæiske Union har også allerede taget vigtige skridt til at opbygge en demokratisk modstandsdygtighed i Europa, herunder med den nye europæiske databeskyttelsesramme, der har været på plads siden maj i år. Denne generelle forordning om databeskyttelse, som nu gælder umiddelbart i hele Den Europæiske Union, rummer de nødvendige værktøjer til at imødegå tilfælde af ulovlig anvendelse af personoplysninger i forbindelse med afholdelse af valg. Der arbejdes også på at fremme et mere sikkert onlinemiljø ved at øge vores samlede

⁴ Jf. den foreløbige rapport, der er offentliggjort af UK Data Protection authority (ICO), efter at der er iværksat en formel undersøgelse af anvendelsen af dataanalyser til politiske formål på baggrund af, at der blev fremsat påstande om ulovlig databehandling og mikromålretning af politisk reklame i forbindelse med folkeafstemningen om EU (<https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf>). I rapporten fremhæves det, at den "hastige sociale og teknologiske udvikling i anvendelsen af big data indebærer, at der er begrænset viden om — eller gennemsigtighed omkring — databehandlingsteknikker bag kulisserne (herunder algoritmer, analyse, datamatching og profilering), der anvendes af organisationer og virksomheder til mikromålretning mod enkeltpersoner. Det står klart, at disse værktøjer kan have en betydelig indvirkning på borgernes privatliv. Det er vigtigt at opnå større og reel gennemsigtighed i brugen af sådanne teknikker for at sikre, at folk har kontrol over deres egne data, og at loven håndhæves. Når formålet med at bruge disse teknikker er knyttet til den demokratiske proces, er der et meget udtalt behov for høje standarder for gennemsigtighed". Det væsentlige i at integrere databeskyttelseshensyn bedre i de bredere lovrammer for valg fremhæves ligeledes.

⁵ Inden for rammerne af EU-retten og deres internationale forpligtelser.

⁶ Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Rapport om valget til Europa-Parlamentet i 2014 (COM(2015) 206 final).

modstandsdygtighed over for cybertrusler, herunder desinformation på nettet og adfærdsmanipulation.

Det er vigtigt at have så stor klarhed som muligt om, hvordan de europæiske databeskyttelsesregler skal gennemføres i denne nye kontekst, samtidig med at vi må optrappe indsatsen for at øge bevågenheden, gennemsigtigheden og sikkerheden. Borgerne bør kunne gennemskue, hvem der taler til dem online, via reklamer og politiske budskaber, og hvem der betaler for politiske reklamer eller politiske budskaber. En vejledning i, hvordan de nye databeskyttelsesregler skal gennemføres i forbindelse med valget til Europa-Parlamentet, forventes at bidrage til større klarhed og lette forståelsen, idet mere samarbejde og udveksling af oplysninger mellem de kompetente myndigheder m.fl. bidrager til at styrke sikkerheden.

Pakken til styrkelse af den demokratiske modstandsdygtighed, der forelægges sammen med denne meddelelse, omfatter afbalancerede, omfattende og målrettede foranstaltninger til støtte for integriteten og den effektive gennemførelse af valget i 2019 til Europa-Parlamentet. Dette er et ansvar, som alle de aktører, der medvirker i valgprocessen, er fælles om. Det kræver konstant årvågenhed og fleksibel tilpasning til et dynamisk miljø og ny teknologisk udvikling. Ved at opstille retningslinjer, henstillinger og nødvendige værktøjer kan europæiske og nationale politiske partier, nationale regeringer, myndigheder, private enheder og interessenter arbejde sammen med større klarhed om at skabe et mere sikkert demokratisk miljø og lige vilkår.

Medlemsstaterne opfordres ligeledes til at anvende principperne i forbindelse med andre valg og folkeafstemninger, som de tilrettelægger på nationalt plan.

De foranstaltninger, der foreslås i denne pakke, tager sigte på at:

1. yde specifik vejledning angående behandlingen af personoplysninger i forbindelse med valg
2. anbefale bedste praksis for at imødegå risici som følge af desinformation og cyberangreb og fremme onlinegennemsigtighed og -ansvarlighed i EU's valgproces og styrke samarbejdet mellem de kompetente myndigheder og indføre de redskaber, der giver dem mulighed for at gribe ind og om nødvendigt indføre sanktionsmuligheder for at beskytte valgprocessens integritet
3. håndtere situationer, hvor politiske partier eller tilknyttede fonde drager fordel af praksis, der overtræder databeskyttelsesreglerne, med henblik på bevidst at påvirke eller søge at påvirke udfaldet af valg til Europa-Parlamentet.

Med forelæggelsen af denne pakke har Kommissionen bestræbt sig på at undgå dels unødvendige administrative byrder, dels på uhensigtsmæssig vis at begrænse de europæiske, regionale og nationale politiske partiers og fondes råderum.

1. EU's nuværende forsvar for at beskytte frie og retfærdige valg

Unionen har allerede taget vigtige skridt til at beskytte integriteten af valg og styrke den demokratiske proces.

Med den generelle forordning om databeskyttelse⁷, som den 25. maj 2018 blev umiddelbart gældende i hele Unionen, råder Den Europæiske Union nu over redskaber, hvormed den kan bidrage til at forebygge og behandle sager om ulovlig anvendelse af personoplysninger. Den Europæiske Union har sat standarden på dette område.

Akten om valg af medlemmerne af Europa-Parlamentet er for nylig ændret, bl.a. med henblik på at øge gennemsigtigheden i forbindelse med valg til Europa-Parlamentet⁸. Den reviderede forordning om statut for og finansiering af europæiske politiske partier⁹, der blev vedtaget den 3. maj 2018, øger de europæiske politiske partiers og de europæiske politiske fondes status, effektivitet, gennemsigtighed og ansvarlighed. I Kommissionens henstilling (EU) 2018/234¹⁰ fremhæves centrale tiltag med henblik på yderligere at effektivisere gennemførelsen af valget til Europa-Parlamentet i 2019.

Europa-Parlamentets og Rådets direktiv 2002/58/EF¹¹ (direktiv om databeskyttelse inden for elektronisk kommunikation) finder anvendelse på uanmodede henvendelser med henblik på direkte markedsføring, herunder politiske meddelelser fra politiske partier og andre aktører, der er involveret i den politiske proces. Det sikrer ligeledes fortroligheden af og beskytter oplysninger, som er lagret i en brugers terminaludstyr såsom en smartphone eller en computer¹². Den foreslåede forordning om databeskyttelse inden for elektronisk kommunikation¹³, som i øjeblikket foreligger til forhandling, vil styrke borgernes kontrol yderligere ved at øge gennemsigtigheden og udvide omfanget af beskyttelsen til ud over traditionelle teleoperatører at omfatte internetbaserede elektroniske kommunikationstjenester.

Desuden har Kommissionen for nylig fremlagt en europæisk strategi til håndtering af desinformation på internettet i sin meddelelse af 26. april 2018¹⁴. Med denne meddelelse søger Kommissionen at fremme et mere gennemsigtigt, troværdigt og ansvarligt onlinemiljø. Et af de vigtigste mål er at udvikle en ambitiøs **adfærdskodeks om desinformation**, som

⁷ 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).

⁸ Rådets afgørelse (EU, Euratom) 2018/994 af 13. juli 2018 om ændring af akten om almindelige direkte valg af medlemmerne af Europa-Parlamentet knyttet til Rådets afgørelse 76/787/EKSF, EØF, Euratom af 20. september 1976 (<https://eur-lex.europa.eu/legal-content/da/TXT/?uri=CELEX:32018D0994&qid=1531826494620>).

⁹ Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 1141/2014 af 22. oktober 2014 om statut for og finansiering af europæiske politiske partier og europæiske politiske fonde (EUT L 317 af 4.11.2014, s. 1).

¹⁰ Kommissionens henstilling (EU) 2018/234 af 14. februar 2018 om en mere synlig europæisk dimension og en mere effektiv gennemførelse af valget til Europa-Parlamentet i 2019 (EUT L 45 af 17.2.2018, s. 40).

¹¹ 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).

¹² Der kræves brugersamtykke, før webstederne kan få adgang til sådanne oplysninger eller spore en brugers adfærd på nettet, f.eks. ved at lagre cookies på brugerens enhed.

¹³ 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).

¹⁴ Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget — Bekæmpelse af desinformation på internettet: en europæisk tilgang" (COM(2018) 236 final).

bl.a. bør forpligtede onlineplatforme og reklamebranchen til at sørge for gennemsigtighed og begrænse mulighederne for at målrette politisk reklame¹⁵. Kodeksen forventes offentliggjort i september 2018¹⁶ og bør give målbare resultater senest i oktober.

Underskriverne af adfærdskodeksen bør nærmere bestemt påtage sig at tage reklameindtægter fra "bedrageriske" websteder og websteder, der hoster desinformation, sørge for gennemsigtighed i forbindelse med sponsoreret indhold, navnlig hvad angår politisk og emnebaseret reklame, etablere tydelige systemer for mærkning af og regler for bots¹⁷ for at sikre, at deres aktiviteter ikke kan forveksles med menneskelig interaktion, og intensivere indsatsen for at lukke falske konti. Underskriverne bør også indvillige i at lette brugernes vurdering af indhold ved at tilskynde til udvikling af indikatorer for pålidelighedsgraden af kilder til indhold, udvande synligheden af desinformation ved at gøre det nemmere at finde troværdigt indhold og oplyse brugerne om prioriteringen af indholdet ved hjælp af algoritmer. Underskriverne bør desuden give betroede organisationer, der arbejder med faktatjek, og den akademiske verden adgang til platformdata. En vurdering af adfærdskodeksen vil indgå i arbejdet med at udarbejde en handlingsplan med konkrete forslag til en koordineret EU-indsats over for desinformation, som skal forelægges af Kommissionen og den højtstående repræsentant inden årets udgang.

For så vidt angår mere "traditionelle" cyberhændelser, f.eks. hacking af IT-systemer eller hærværk mod websteder, er definitionerne af strafbare handlinger og minimumsniveauet for de maksimale strafferetlige sanktioner for angreb på informationssystemer blevet harmoniseret på EU-plan ved direktiv 2013/40/EU om angreb på informationssystemer.

Den samarbejdsgruppe, der er nedsat ved Europa-Parlamentets og Rådets direktiv (EU) 2016/1148¹⁸, har udpeget cybersikkerhed i forbindelse med valg som en fælles udfordring. Samarbejdsgruppen, som omfatter de nationale kompetente myndigheder med ansvar for cybersikkerhed, Kommissionen og Den Europæiske Unions Agentur for Net- og Informationssikkerhed ("ENISA"), har kortlagt eksisterende nationale initiativer vedrørende cybersikkerhed for net- og informationssystemer, der anvendes ved valg. Den har peget på risici, der er knyttet til en utilstrækkelig grad af cybersikkerhed, og som kunne påvirke næste valg til Europa-Parlamentet, og den har udarbejdet et kompendium om cybersikkerhed i forbindelse med valgteknologi, herunder tekniske og organisatoriske foranstaltninger baseret på erfaringer og bedste praksis. Kompendiet rummer praktisk vejledning for cybersikkerhedsmyndigheder og organer med ansvar for gennemførelse af valg.

¹⁵ Med henblik på at udarbejde denne adfærdskodeks indkaldte Kommissionen i maj 2018 til et forum bestående af en "arbejdsgruppe" (med deltagelse af de største onlineplatforme og repræsentanter for reklamebranchen og større annoncører) og en gruppe af sparringspartnere (bestående af en række repræsentanter for medierne og civilsamfundet).

¹⁶ Efter at sparringspartnere afgav deres udtalelse.

¹⁷ Bots omfatter automatiske beskeder på sociale medieplatforme og mere interaktive applikationer som f.eks. chatbots, der kommunikerer direkte med brugerne.

¹⁸ Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

2. Yderligere styrkelse af den demokratiske modstandsdygtighed: forbedring af samarbejdsnetværk, gennemsigtighed online, beskyttelse mod cybersikkerhedshændelser og bekæmpelse af desinformationskampagner i forbindelse med valg til Europa-Parlamentet

I betragtning af udfordringens omfang og da det formelle ansvar på dette område er delt mellem flere myndigheder, vil der kun blive opnået meningsfulde resultater, hvis alle de relevante aktører arbejder sammen.

Denne meddelelse ledsages af en henstilling om valgsamarbejdsnetværk, gennemsigtighed online, beskyttelse mod cybersikkerhedshændelser og bekæmpelse af desinformationskampagner i forbindelse med valg til Europa-Parlamentet. For at sikre frie og retfærdige valg bør denne henstilling gennemføres af alle aktører i god tid forud for valget i 2019 til Europa-Parlamentet.

I henstillingen opfordrer vi hver medlemsstat til at oprette og støtte et nationalt valgnetværk. Medlemsstaternes myndigheder med kompetence i valgspørgsmål bør rettidigt og effektivt samarbejde med myndigheder på tilknyttede områder (såsom databeskyttelsesmyndigheder, medietilsynsmyndigheder, cybersikkerhedsmyndigheder osv.). Om nødvendigt bør de også samarbejde med de retshåndhævende myndigheder. Det vil sætte dem i stand til hurtigt at afsløre potentielle trusler mod valg til Europa-Parlamentet og hurtigt håndhæve eksisterende regler, herunder eventuelle finansielle sanktioner såsom tilbagebetaling af det offentlige bidrag. Unionens og medlemsstaternes lovgivning skal overholdes og håndhæves. Med dette for øje opfordrer Kommissionen medlemsstaterne til i overensstemmelse med gældende national ret og EU-ret at fremme udveksling af oplysninger fra databeskyttelsesmyndighederne til myndigheder med ansvar for at overvåge valg og overvåge politiske partiers aktiviteter og finansiering, hvis det følger af deres afgørelser, eller hvis der er andre rimelige grunde til at antage, at en overtrædelse er knyttet til politiske aktiviteter, der udøves af nationale politiske partier eller fonde i forbindelse med valg til Europa-Parlamentet.

Der henstilles ligeledes til, at medlemsstaterne udpeger kontaktpunkter med henblik på at deltage i et europæisk samarbejdsnetværk for valg til Europa-Parlamentet. Kommissionen vil støtte disse samarbejdsnetværk ved at indkalde til et første møde mellem de udpegede kontaktpunkter senest i januar 2019. Under hensyntagen til de nationale kompetencer og de procedurekrav, der gælder for de berørte myndigheder, vil dette forum udgøre kernen i en tidstro europæisk varslingsproces og et forum for udveksling af oplysninger og praksis mellem medlemsstaternes myndigheder.

Politiske partier, fonde og kampagneorganisationer vil skulle garantere en gennemsigtig praksis med hensyn til deres politiske kommunikation til borgerne og sørge for, at den europæiske valgproces ikke fordrejes af illoyal praksis. Kommissionen forelægger konkrete foranstaltninger for at øge gennemsigtigheden, så borgerne kan se, hvem der står bag den

politiske kommunikation, de modtager, og hvem der betaler for den¹⁹. Medlemsstaterne bør støtte og fremme en sådan gennemsigtighed og de kompetente myndigheders bestræbelser på at overvåge overtrædelser og håndhæve regler, herunder om fornødent ved at pålægge sanktioner. Hvis det er relevant, bør de retshåndhavende myndigheder også inddrages for at sikre en passende reaktion på hændelser og anvendelsen af passende strafferetlige sanktioner²⁰.

Modstandsdygtighed, afskrækkelse og forsvar er afgørende for at opbygge en solid cybersikkerhed i Den Europæiske Union²¹. Kompetente europæiske og nationale myndigheder, politiske partier, fonde og kampagneorganisationer bør være fuldt ud opmærksomme på risiciene ved næste års valg og anvende egnede midler til at beskytte deres net og informationssystemer²².

3. Anvendelse af databeskyttelsesregler i forbindelse med valgprocessen

Europa-Parlamentets og Rådets forordning (EU) 2016/679 (generel forordning om databeskyttelse)²³, 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 afholdelse af valg.

Da disse regler for allerførste gang vil blive anvendt ved et valg på EU-plan i forbindelse med det kommende valg til Europa-Parlamentet, er det vigtigt, at alle de aktører, som medvirker i valgprocessen — såsom nationale valgmyndigheder, politiske partier, datamæglere og dataanalytikere, sociale medieplatforme og onlinereklame-netværk — forstår, hvordan reglerne bedst kan anvendes, og hvad der ifølge dem er eller ikke er tilladt.

¹⁹ Disse forslag supplerer adfærdskodeksen, der udarbejdes af det multiinteressentforum, som Kommissionen har sammenkaldt efter dens meddelelse af 26. april 2018 om desinformation online.

²⁰ Dette vil navnlig vedrøre sager, hvor ondsindet indhold målrettes mod en valgproces, herunder hændelser med baggrund i angreb på informationssystemer. Alt efter omstændighederne kan det være hensigtsmæssigt at indlede en strafferetlig efterforskning, der kan udmønte sig i strafferetlige sanktioner. Som nævnt ovenfor er definitionerne af strafbare handlinger og minimumsniveauet for de maksimale strafferetlige sanktioner for angreb på informationssystemer blevet harmoniseret ved direktiv 2013/40/EU.

²¹ I den fælles meddelelse af september 2017 fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og Europa-Kommissionen anerkendes behovet for en samlet reaktion med henblik på at opbygge en solid cybersikkerhed i Unionen, som er baseret på modstandsdygtighed, afskrækkelse og forsvar (JOIN(2017) 450 final).

²² Kompendiet, som er udarbejdet af den samarbejdsgruppe, der er nedsat i medfør af direktiv (EU) 2016/1148, indeholder nyttige retningslinjer i denne henseende. Med direktiv (EU) 2016/1148 tilsigtes det at opnå et højt fælles niveau for modstandsdygtighed med hensyn til cybersikkerhed i hele Unionen. For at nå dette mål støtter direktivet udviklingen af nationale cybersikkerhedskapaciteter og beskytter tilvejebringelsen af væsentlige tjenester i nøglesektorer. For at styrke indsatsen med henblik på at gennemføre direktivet korrekt stiller Kommissionen over 50 mio. EUR til rådighed frem til 2020 via Connecting Europe-faciliteten (CEF). Risikostyringsforanstaltningerne i direktiv (EU) 2016/1148 er relevante benchmarks for valgprocessen. Ved den generelle forordning om databeskyttelse fastsættes også forpligtelser til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sørge for et sikkerhedsniveau for personoplysninger, som behandles. Den finder anvendelse på alle de aktører, der medvirker i valgprocessen, og indeholder også en forpligtelse til at underrette de kompetente databeskyttelsesmyndigheder og de berørte enkeltpersoner om brud på persondatasikkerheden (jf. Kommissionens vejledning).

²³ 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).

Kommissionen har derfor udarbejdet specifikke retningslinjer for at sætte fokus på de databeskyttelsesforpligtelser, der er relevante i forbindelse med valg. For at bekæmpe ondsindede forsøg på at misbruge personoplysninger, navnlig med henblik på mikromålretning, skal nationale databeskyttelsesmyndigheder som håndhævere af den generelle forordning om databeskyttelse gøre fuld brug af deres styrkede beføjelser til at imødegå eventuelle overtrædelser.

4. Styrkelse af finansieringsreglerne for de europæiske politiske partier

Politiske partier og fonde er naturligvis de vigtigste aktører i forbindelse med valg. De konkurrerer om vælgernes stemmer gennem deres kampagner. For at sikre lige vilkår i valgkampen og for at beskytte alle politiske partier og fonde mod ulovligheder er det vigtigt at forebygge situationer, hvor et af partierne kan drage fordel af ulovlig praksis, der overtræder databeskyttelsesreglerne. Ulovlig praksis, som ikke blot krænker borgernes ret til privatliv og fred, men som potentielt også kan påvirke udfaldet af valg til Europa-Parlamentet, bør straffes. Sideløbende med en opfordring til medlemsstaterne om at pålægge partier og fonde sanktioner på nationalt plan, hvis det er relevant, foreslår Kommissionen at indføre en målrettet ændring af forordning (EU, Euratom) nr. 1141/2014 med henblik på at fastsætte forholdsmæssigt afpassede sanktioner i sager, der involverer politiske partier og fonde på europæisk plan. En sådan ændring, der styrker de eksisterende regler, har til formål at sikre, at valg til Europa-Parlamentet kan holdes under overholdelse af strenge demokratiske regler og med fuld respekt for de værdier, som Unionen bygger på, navnlig demokrati, grundlæggende rettigheder og retsstatsprincippet.

Kommissionen opfordrer Europa-Parlamentet og Rådet til at sørge for, at disse målrettede ændringer indføres inden valget til Europa-Parlamentet i 2019.

5. Konklusion

Det fremgår af de seneste begivenheder, at risikoen for manipulation af valgprocessen, uanset om det sker via angreb på informationssystemer, misbrug af personoplysninger eller uigennemsigtig praksis, er reel og akut. EU er ikke immun. Onlineaktiviteter i forbindelse med afholdelse af valg udgør en ny trussel og kræver særlig beskyttelse. Borgernes og demokratiets interesser tjener vi bedst ved at forberede os nu. Vi bør ikke vente til efter afholdelsen af valg eller folkeafstemninger med at konstatere, om sådanne aktiviteter har fundet sted og så først reagere på dem til den tid.

Den Europæiske Union og dens medlemsstater har et fælles ansvar, som bør tages meget alvorligt, for at beskytte demokratiet i Unionen. Det haster. Alle medvirkende aktører må øge deres indsats og samarbejde for at afskrække fra, forebygge og straffe ondsindet indgriben i

valgssystemet. De foranstaltninger, som Kommissionen har foreslået i denne pakke, støtter disse bestræbelser.

Kommissionen vil efter valget i 2019 aflægge rapport til Europa-Parlamentet om gennemførelsen af denne pakke af foranstaltninger.

De næste skridt forud for valget til Europa-Parlamentet i 2019

- *Kommissionen opfordrer Europa-Parlamentet og Rådet til at sørge for, at disse målrettede ændringer af forordning (EU, Euratom) nr. 1141/2014 indføres i rette tid til valget til Europa-Parlamentet i 2019.*
- *Sammen med den højtstående repræsentant vil Kommissionen støtte udarbejdelsen af en fælles europæisk reaktion på en eventuel udenlandsk indgriben i valg i Den Europæiske Union²⁴. Som opfølgning på Det Europæiske Råds konklusioner fra juni 2018 vil der i samarbejde med medlemsstaterne blive fremlagt en handlingsplan senest i december 2018 med specifikke forslag til en koordineret EU-reaktion på den udfordring, som desinformation indebærer.*
- *Kommissionen vil øge bevågenheden og opretholde sin dialog med medlemsstaternes myndigheder via konferencen på højt niveau om cyberbaserede trusler mod valget den 15. og 16. oktober 2018, hvis udfald vil indgå i det næste kollokvium om grundlæggende rettigheder (26. og 27. november 2018) med fokus på "Demokrati i Den Europæiske Union".*

²⁴ Dette kunne også omfatte anvendelsen af de foranstaltninger, der er udviklet under rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter.