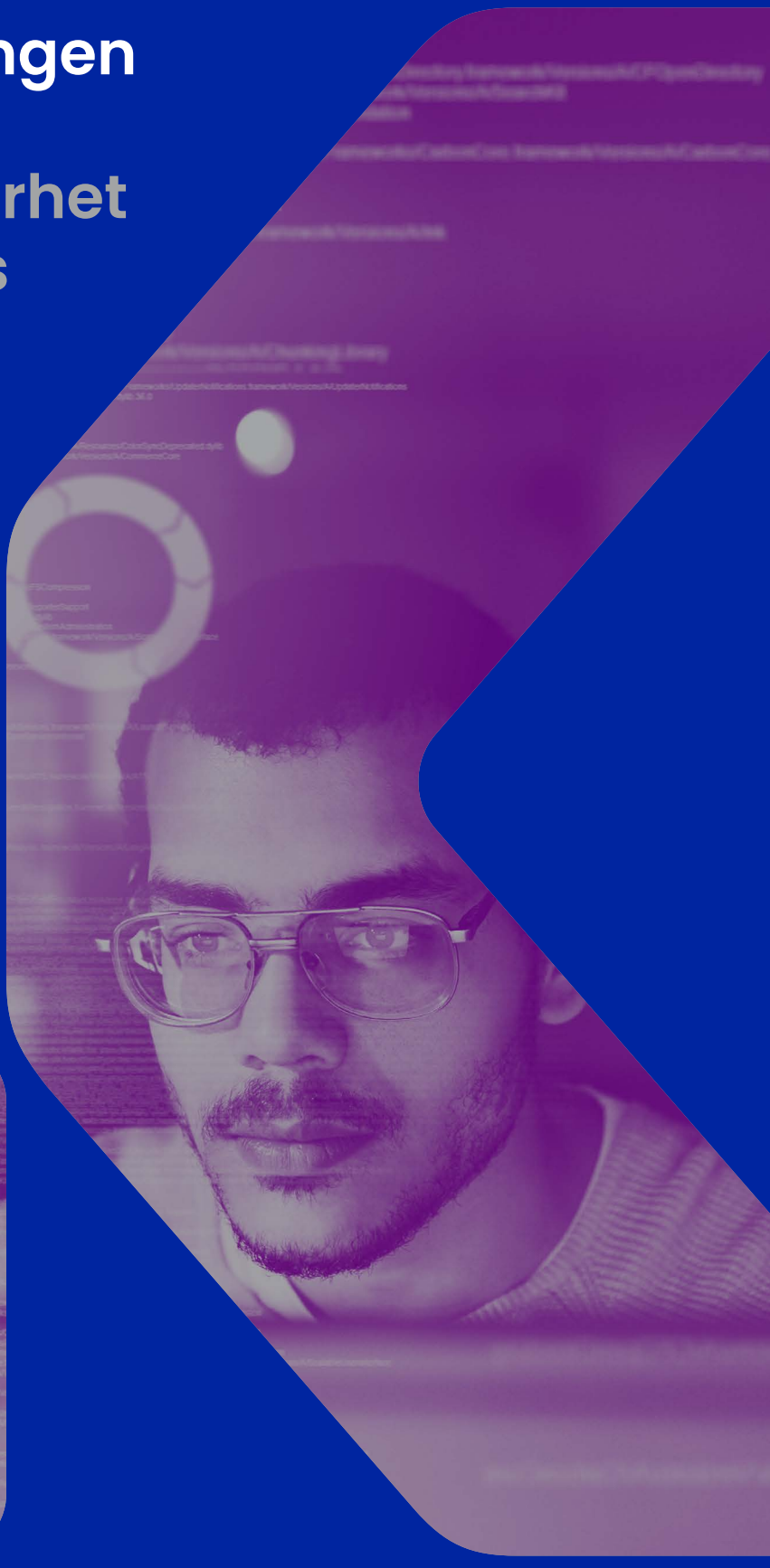
Direktoratet for høyere utdanning og kompetanse

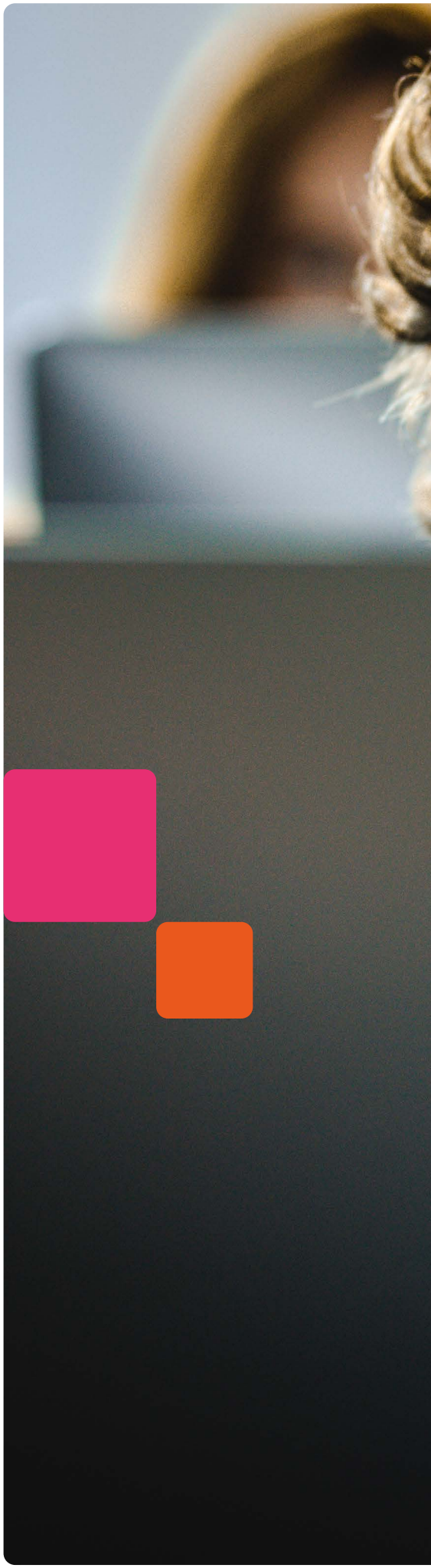
Temarapport 2021

# Pandemihåndteringen – betydningen for informasjonssikkerhet og personvern hos universiteter og høgskoler




01001100011011110
11100100110010101
10110100100000011
01001011100000111
00110111010101101
10100100000011001

# Innhold



# Sammendrag

## I denne temarapporten ser vi på hvordan pandemien og korona-nedstenginger påvirket arbeidet med informasjonssikkerhet og personvern hos de 21 statlige universitetene og høgskolene.

I rapporten drøftes ulike problemstillinger knyttet til pandemi-situasjonen: førte den til flere uønskede hendelser enn tidligere, ble det tatt i bruk nye IT-løsninger, hvordan ble det systematiske arbeidet med informasjonssikkerhet og person-vern påvirket, ble det iverksatt ekstraordinære sikring- og personverntiltak og hvilke personvernutfordringer måtte håndteres?

Funnene og drøftelsene i rapporten baserer seg på Unit/ HK-dir sin kartlegging av informasjonssikkerhet og personvern i UH-sektoren for 2021.

**Hovedkonklusjonene i rapporten er som følger:**

- Korona-nedstengningene har ikke ført til en vesentlig økning i antallet uønskede informasjonssikkerhets- og personvernhendelser. Trusselbildet i sektoren er likevel blitt mer utfordrende, men vi har ikke grunnlag for å knytte dette til pandemisituasjonen.

- Med unntak av kommunikasjons- og samhandlingsplattformene Zoom og Teams, ble det ikke tatt i bruk mange nye digitale systemer eller -tjenester i forbindelse med pandemihåndteringen. De største endringene handlet om kraftige økninger i bruksvolum for eksisterende og enkelte nye IT-løsninger og hvordan løsningene ble brukt.

- Hos flertallet av universitetene og høgskolene oppsto det et etterslep i arbeidet med innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet og internkontroll for personvern (GDPR). Dette etterslepet må hentes inn igjen nå som situasjonen er i ferd med å normalisere seg.

- Det ble iverksatt en rekke ekstraordinære informasjonssikkerhets- og personverntiltak i forbindelse med pandemihåndteringen (tekniske, organisatoriske og pedagogiske). Mange av tiltakene vil trolig være relevante også etter at pandemien er over.

- Hjemmekontor og digital undervisning reiste flere typer utfordringer på personvernområdet. De viktigste av disse gjaldt digital kommunikasjon og samhandling, digitale verktøy i forskning og bruk av privat IT-utstyr, hjemmedatanettverk og webkamera.

Universitetene og høgskolene synes å ha håndtert informasjonssikkerhet og personvern på en tilfredsstillende måte under pandemien. Unit/HK-dir sine årlige risiko- og tilstandsvurderinger indikerer imidlertid at trusselbildet i sektoren er mer utfordrende enn tidligere. Samtidig har sektorens avhengighet av digitale løsninger økt og det har oppstått et visst etterslep i arbeidet med ledelsessystemer og internkontroll.

Det er derfor viktig at universiteter og høgskoler – og øvrige virksomheter i UH-sektoren – fortsetter og forsterker det systematiske arbeidet med informasjonssikkerhet og personvern.

# Innledning

## Korona-nedstenginger verden over våren 2020 førte raskt til spekulasjoner om hvilke konsekvenser den plutselige «unntaks-tilstanden» kunne få for informasjons-sikkerheten og personvernet.[1]

Kan behovet for å holde samfunnshjulene i gang i for stor grad gå på bekostning av sikkerheten til nye og gamle IT-løsninger? I hvilken utstrekning vil hjemmearbeid, bruk av privat IT-utstyr, tilgang til IT-systemer over usikre datanettverk, svak autentisering og liten fysisk kontakt mellom kollegaer gjøre oss mer sårbare for nettsvindel, datainntrenging og utpressingsvare? Hvor godt vil statlige hackere og nettkriminelle aktører lykkes med å utnytte sikkerhetshull i hastig innførte IT-løsninger til datatyveri og -spionasje?

Dette var bekymringer også i høyere utdanning og forskning, spesielt knyttet til hjemmekontor, digital eller hybrid undervisning, lærings-plattformer og andre typer kommunikasjons- og samhandlings-tjenester.[2] Enkelte internasjonale studier tyder på at bekymringene ikke var helt grunnløse – kunnskapssektoren har i perioder under pandemien vært særlig utsatt for dataangrep og forsøk på datainntreng-ing.[3] I andre og tilsvarende studier er ikke dette en like tydelig trend.[4]

I denne temarapporten retter vi blikket mot norsk UH-sektor. Vi drøfter i hvilken grad og på hvilke måter arbeidet med informasjonssikkerhet og personvern hos de 21 statlige universitetene og høgskolene ble påvirket av pandemi-nedstengningen 12. mars 2020.

### Vi diskuterer særlig følgende spørsmål:

- Førte nedstengingen til en økning i antallet brudd på informasjonssikkerheten og krenkelser av personvernet hos universitetene og høgskolene?
- Innførte universitetene og høgskolene mange nye digi-tale systemer eller tjenester for fortsatt å kunne utføre sine kjerneoppgaver?
- Hvordan ble arbeid med ledelsessystemer for informa-sjonssikkerhet og internkontroll for personvern (GDPR) påvirket av nedstengingen?
- Hvilke ekstraordinære informa-sjonssikkerhets- eller person-verntiltak ble iverksatt i for-bindelse med nedstengingen?
- Hva var de vanligste personvern-utfordringene som ble diskutert og håndtert i kjølvannet av nedstengingen?

1 Se for eksempel Verizons spesialrapport om Covid-19 og informasjonssikkerhet, oktober 2020 (https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/).

2 Se for eksempel Kaspersky (2021): Digital Education: the Cyberrisks of the Online Classroom (https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/03172621/education_report_04092020.pdf).

3 Se for eksempel Check Point (2021): Education Sector Sees 29 % Increase in Attacks Against Organizations Globally (https://blog.checkpoint.com/2021/08/18/check-point-research-education-sector-sees-29-increase-in-attacks-against-organizations-globally/).

4 Se for eksempel Fireeye/Mandiant (2021): M-Trends 2021 (https://www.mandiant.com/resources/m-trends-2021).

## Datagrunnlaget

Denne temarapporten baserer seg på funn fra Unit/HK-dir sin kartlegging av informasjons-sikkerhet og personvern i UH-sektoren for 2021. Kart-leggingen omfatter alle de 21 statlige universitetene og høgskolene.

Kartleggingen ble gjennomført i perioden januar-mars 2021, det vil si 10-12 måneder etter ned-stengingen 12. mars 2020. Den fanger derfor opp alle viktige endringer på informasjons-sikkerhets- og personvern-området hos universitetene og høgskolene etter at korona-nedstengingen ble iverksatt.

Datagrunnlag og metodikk gjøres nærmere rede for i «Risiko- og tilstandsvurdering 2021», vedlegg 1-3.[5]

5 Unit (2021): Risiko- og tilstandsvurdering 2021 (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

# Flere sikkerhetsbrudd og personvernkrenkelser?

I Unit/HK-dir sin siste kartlegging av informasjonssikkerhet og personvern i UH-sektoren,[6] ble universitetene og høgskolene bedt om å oppgi antall og typer brudd på informasjonssikkerheten og krenkelser av personvernet registrert i 2020. Samlet sett viser svarene fra institusjonene at antallet slike brudd og krenkelser ikke var høyere i pandemi- og nedstengingsåret 2020 enn i 2019 og 2018.

## HENDELSER MELDT TIL DATATILSYNET

Institusjonene rapporterte likevel om en dobling i antallet hendelser som ble meldt til Datatilsynet sammenliknet med 2019. Hendelsene gjaldt i hovedsak brudd på personopplysningssikkerheten som følge av menneskelige feil (feilsending av eposter, feil publisering eller lagring av dokumenter, osv.).

Det kan tenkes at enkelte av hendelsene skyldes at rutiner for håndtering av personopplysninger i mindre grad ble overholdt når ledere og medarbeidere jobber hjemmefra enn når de jobber på kontoret. Men det kan også tenkes at økningen skyldes at flere hendelser ble oppdaget og meldt, eventuelt begge deler.

## FLERE ALVORLIGE HENDELSER

Institusjonene rapporterte om noen flere alvorlige digitale sikkerhetshendelser i 2020 enn tidligere, for eksempel at datanettverket hos enkelte institusjoner hadde blitt kompromittert. For enkelte av hendelsene kunne både oppdagelses- og reparasjonstiden være lang.

Vi kan ikke utelukke at disse informasjonssikkerhets- og personvernhendelsene kunne vært unngått i en normalsituasjon, men vi har heller ikke grunnlag for å knytte dem til korona-nedstengingen. Hendelsene kan like gjerne skyldes tilfeldigheter, et generelt skjerpet trusselbilde (uavhengig av pandemien) eller systematiske mangler i det lokale arbeidet med informasjonssikkerhet og personvern.

## SIKKERHETSOVERVÅKNING I SEKTOREN

Uninett AS har verktøy for å oppdage mistenkelig og uønsket aktivitet i forskningsnettet. Selskapet opplyste om at det var registrert noen flere digitale sikkerhetshendelser i forskningsnettet i 2020 enn i 2019. Antallet hendelser var likevel lavere enn i 2018.

Både NTNU og UiO har egne verktøy og ekspertmiljøer for oppdagelse, analyse og håndtering av digitale sikkerhetshendelser i sine lokale datanettverk. Heller ikke de rapporterte om vesentlige økninger i slike hendelser i 2020 sammenliknet med tidligere år.

## SAMLET VURDERING

Oppsummert kan vi si at korona-nedstengingen ikke har medført en vesentlig økning i antallet uønskede

6 Se Unit (2021): Risiko og tilstandsvurdering 2021, side 4-6 og kapittel 3 (https://www.unit.no/styring-av-informasjonssikkerhet-og-personvern-i-hoyere-utdanning-og-forskning).

## Internasjonale trender

Siden våren 2020 har det kommet en jevn strøm med internasjonale undersøkelser som indikerer at pandemien og korona-nedstenginger har ført til flere brudd på informasjonssikkerheten og en økning i antallet uønskede personvernhendelser. Noen av de siste rapportene antyder blant annet at

- Covid-19-tematikk benyttes fortsatt hyppig av statlige hackere og nettkriminelle aktører i nettfiske-kampanjer,[8]
- nye pandemi-nedstenginger fører til at individer og virksomheter blir mer sårbare for nettkriminell aktivitet, inkludert løsepengevirus,[9]
- kostnadene ved sikkerhetsbrudd hvor bruk av hjemmekontor og fjerntilgang til IT-systemer er medvirkende faktorer, er høyere enn ved andre typer sikkerhetsbrudd,[10]
- pandemien har bidratt til at statlige eller statsstøttede hackere og nettkriminelle grupper har utviklet nye fremgangsmåter som vil være en trussel også etter at pandemien er over.[11]

I Norge mener Nasjonal Sikkerhetsmyndighet at sårbarheter som ble fremskyndet av pandemien trolig er kommet for å bli.[12] Vi ser ingen særskilte grunner til at dette ikke også gjelder i UH-sektoren. UH-sektoren bør derfor sørge for at sårbarheter utbedres for å unngå fremtidige brudd på informasjonssikkerheten og krenkelser av personvernet.

informasjonssikkerhets- og personvernhendelser. Samtidig rapporterer Nasjonal sikkerhetsmyndighet om at de har registrert tre ganger så mange alvorlige digitale sikkerhetshendelser i 2020 som i 2019.[7] Utviklingen hos universitetene og høgskolene under pandemien synes derfor å avvike noe fra den generelle trenden i samfunnet.

Der hvor vi ser en økning, for eksempel når det gjelder meldinger til Datatilsynet om brudd på personopplysningssikkerheten, har vi ikke klare indikasjoner på at dette skyldes forhold knyttet til pandemien og korona-nedstengingen. Det synes derfor rimelig å anta det skjerpede trusselbildet som beskrives i Unit/HK-dir sin siste risiko- og tilstandsvurdering, spesielt flere alvorlige hendelser med lang oppdagelses- eller reparasjonstid, trolig skyldes andre forhold.

7 NSM (2021): Nasjonalt digitalt risikobilde 2021 (https://nsm.no/getfile.php/137495-1635323653/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf).

8 Proofpoint (2021): As Delta Variant Spreads, COVID-19 Themes Make Resurgence In Email Threats (https://www.proofpoint.com/us/blog/threat-insight/delta-variant-spreads-covid-19-themes-make-resurgence-email-threats?&web_view=true).

9 Reuters, 15. september 2021: Cyber Crime Spreads In Australia As COVID-19 Pushes More People Online (https://www.reuters.com/technology/australia-sees-13-rise-cyber-crime-reports-covid-19-pushes-more-people-online-2021-09-15/).

10 IBM (2021): Cost of Data Breach Report 2021 (https://www.ibm.com/security/data-breach).

11 McAfee og FireEye (2021): 2022 Threat Predictions (https://www.mcafee.com/blogs/enterprise/mcafee-enterprise-atr/mcafee-enterprise-fireeye-2022-threat-predictions/).

12 NSM (2021): Nasjonalt digitalt risikobilde 2021, side 10 (https://nsm.no/getfile.php/137495-1635323653/Demo/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf).

# Nye systemer og tjenester

**For å gjennomføre digital undervisning og legge til rette for hjemmearbeid, kan det tenkes at universitetene og høgskolene hadde behov for å innføre nye digitale systemer eller tjenester.**

I den grad dette skjedde fikk institusjonene en større og mer kompleks IT-portefølje enn før pandemien. Dermed kunne også risikoen for uønskede informasjonssikkerhets- og personvernhendelser øke, spesielt dersom innføringen skjedde raskt og uten at risikoreduserende tiltak ble iverksatt.

Institusjonene ble derfor spurt om nye digitale systemer eller tjenester ble tatt i bruk for å håndtere koronanedstengingen, og hvilke systemer eller tjenester dette i så fall var. Spørsmålet omfattet også hasteinnføring av allerede planlagte system- eller tjenesteanskaffelser.

## OMFANGET AV NYANSKAFFELSER

I figur 1 ser vi at 16 universiteter og høgskoler svarte at nye digitale systemer eller tjenester ble tatt i bruk, eller at planlagte anskaffelser ble hasteinnført.

Fem institusjoner oppga at ingen slike systemer eller tjenester ble innført – og at det heller ikke ble iverksatt hasteinnføring av planlagte anskaffelser. Disse institusjonene var derfor utrustet med det de trengte på IT-siden for å håndtere nedstengingen før den trådte i kraft 12. mars 2020.

## HVILKE SYSTEMER OG TJENESTER?

Når vi ser på hvilke nye digitale systemer og tjenester som ble tatt i bruk eller hasteinnført, dominerer kommunikasjons- og samhandlingsplattformene Zoom og Teams. 13 institusjoner oppga at Zoom ble et nytt tilskudd til deres IT-portefølje som følge av nedstengingen. Tre institusjoner sa det samme om Teams.

I tillegg opplyste enkelte institusjoner om at de hadde innført andre IT-løsninger enn Zoom og Teams, blant annet Snapmonitor, Lola, Jamulus, Mentimeter og CIM.

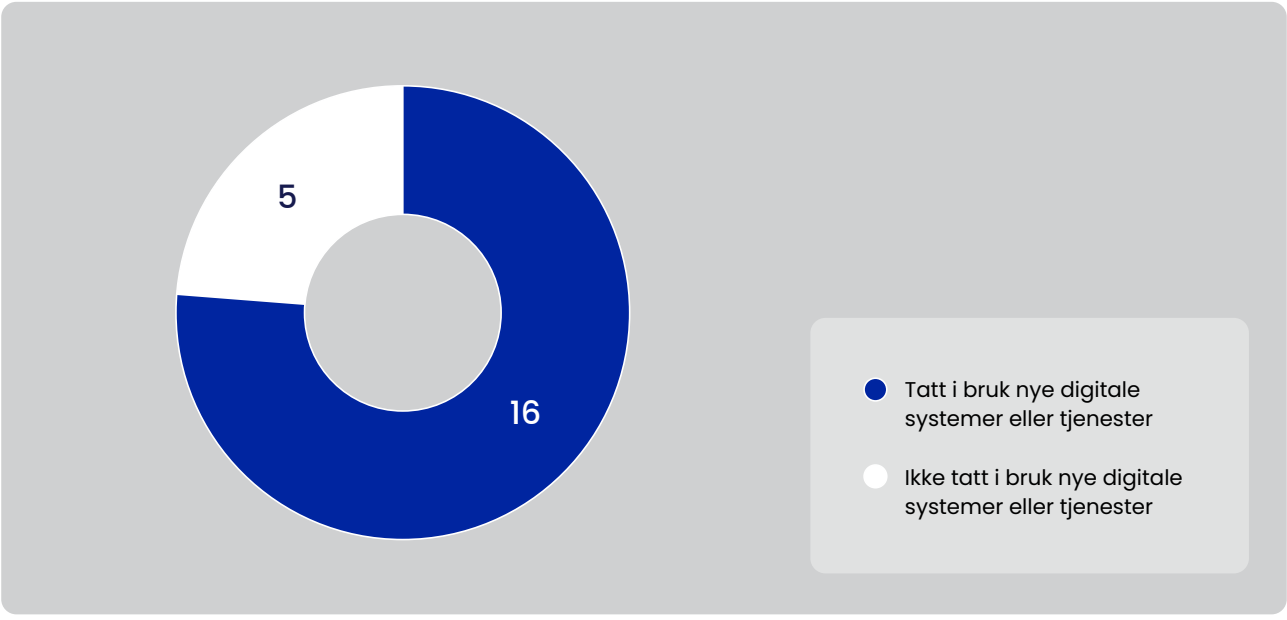
## «SJOKK-DIGITALISERING»

Svarene fra universitetene og høgskolene indikerer at sektoren ikke hadde behov for mange nye IT-løsninger for å håndtere korona-nedstengingen. På system- og tjenestesiden kan vi derfor ikke si at pandemien førte til en «sjokk-digitalisering».

Institusjonene understreket imidlertid at det hadde skjedd store endringer på andre områder. Dette handlet om endrede bruksmønstre og -volum: nedstengingen førte til at IT-løsninger ble anvendt på nye måter og at bruken av kommunikasjons- og samhandlingsplattformer vokste kraftig.

Pandemiens innvirkning på risikoen for uønskede hendelser og avvik synes derfor å handle om endringer i omfanget av og måten IT-løsninger brukes på, snarere enn om at IT-porteføljen i sektoren har blitt vesentlig større og mer kompleks.

Figur 1: Nye digitale systemer eller tjenester



# Ledelsessystemer og internkontroll

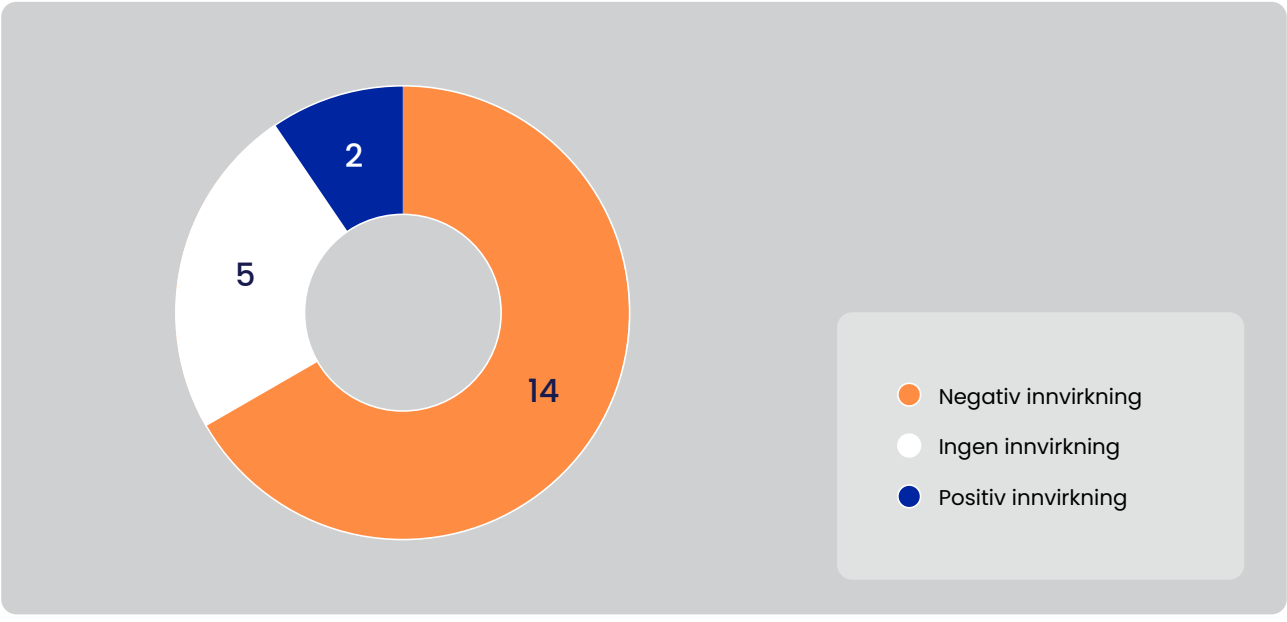
**Selv om korona-nedstenginger av universiteter og høgskoler ikke hadde ført til vesentlige økninger i antallet sikkerhetshendelser og personvernkrenkelser, kan nedstengningene likevel ha påvirket arbeid med ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR).**

Det kan for eksempel tenkes at arbeidet ble forsinket fordi knappe ressurser ble omprioritert til å holde kjernevirksomheten i gang eller at lengre perioder med jobbing på hjemmekontor førte til at det ble vanskelig å gjennomføre planlagte aktiviteter.

Vi spurte derfor universitetene og høgskolene om arbeidet med innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR) hadde blitt påvirket av korona-nedstenginger.

Figur 2 oppsummerer hva institusjonene svarte.

**Figur 2: Innvirkning på arbeidet med ledelsessystemer og internkontroll (GDPR)**



# Ledelsessystemer og internkontroll

Ledelsessystemer strukturerer arbeidet med risikostyring av informasjonssikkerheten. Formålet er at virksomhetene skal oppnå og vedlikeholde et tilfredsstillende sikkerhetsnivå. Et ledelsessystem for informasjonssikkerhet omfatter følgende hovedaktiviteter:

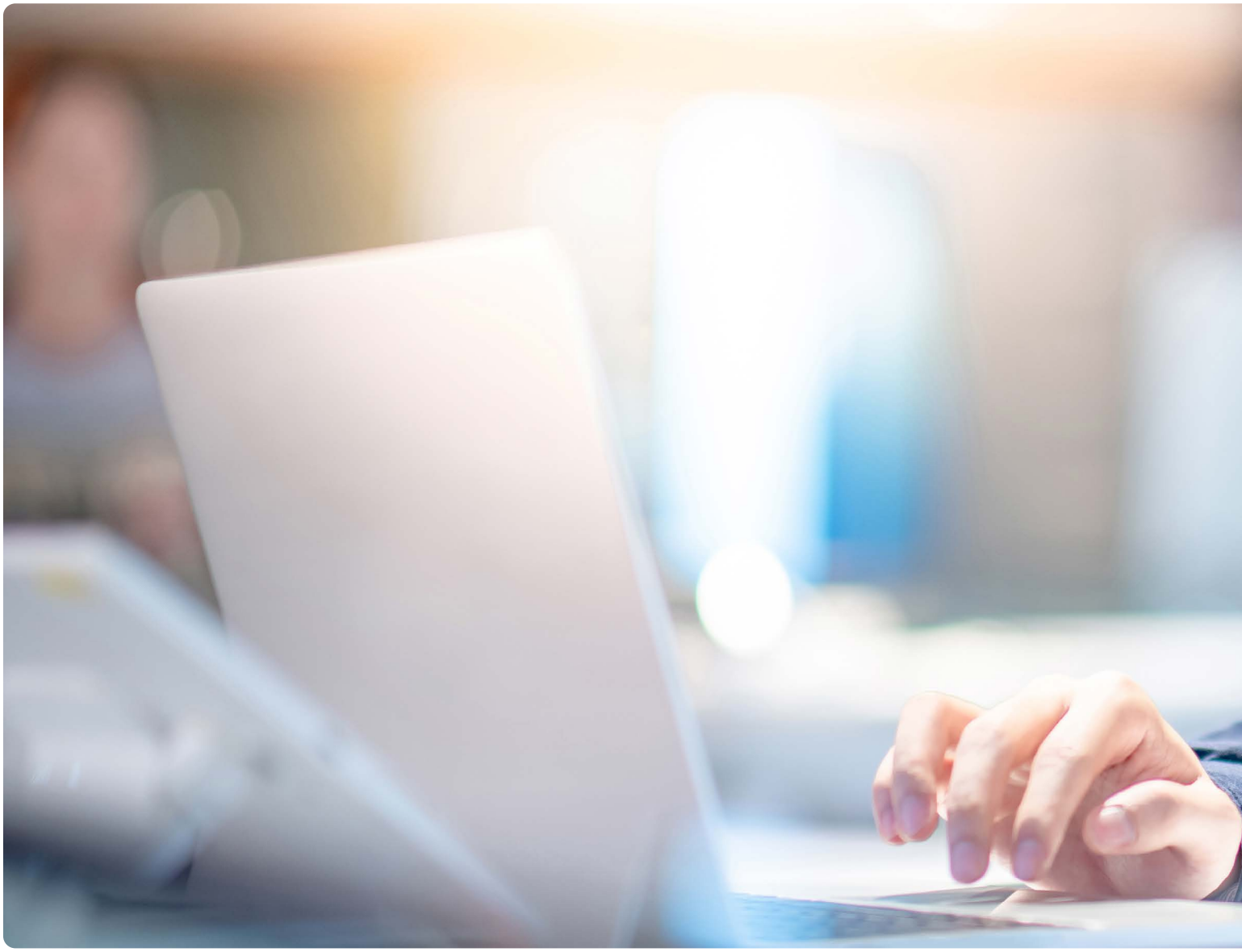
(i) identifisere hva som skal sikres (data, personopplysninger, programvare, data-maskiner, osv.),
(ii) vurdere risikoen for brudd på informasjons-sikkerheten og etablere forebyggende tiltak,
(iii) oppdage og håndtere brudd på infor-masjonssikkerheten og avvik fra egne sikkerhetsrutiner,
(iv) opprettholde kritiske oppgaver/funksjoner ved alvorlige informasjonssikkerhets-hendelser,
(v) gjenopprette sikker drift etter alvorlige informasjonssikkerhetshendelser.

Internkontrollen for personvern (GDPR) skal sørge for at virksomheten jobber systematisk med å overholde sine plikter etter personopplysnings-loven og personvernforordningen. Disse pliktene inkluderer blant annet grunnleggende krav til behandling av personopplysninger (formåls- og lagringsbegrensning, rettslig grunnlag, osv.), krav til personopplysningssikkerhet, ivaretakelse av de registrertes rettigheter, bruk av databehand-lere og overføringer av personopplysninger til tredjeland.

Som ledelsessystemer for informasjonssikkerhet, er internkontrollen for personvern (GDPR) basert på risikostyring og bygd opp på samme måte som andre typer internkontrollsystemer (styrende, gjennomførende og kontrollerende deler).

Øvrige krav til arbeidet med informasjonssikker-het og personvern følger av Kunnskapsdeparte-mentets policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.[13]

13 Policyen er tilgjengelig på https://www.unit.no/styring-av-informasjons-sikkerhet-og-personvern-i-hoyere-utdanning-og-forskning.



## NEGATIV EFFEKT

Figur 2 viser at 14 universiteter og høgskoler opplyste om at korona-nedstenginger hadde hatt en negativ innvirkning på arbeidet med innføring og videreutvikling av ledelsessystemer og internkontroll (GDPR).

Det disse institusjonene særlig nevnte var at planlagte oppgaver hadde blitt utsatt eller avlyst. Det kunne for eksempel dreie seg om aktiviteter knyttet til etablering og innføring av ledelsessystemer og revisjon av internkontrollen (GDPR). Andre oppgaver som ble utsatt eller avlyst inkluderte risikovurderinger av IT-systemer, videreutvikling av beredskaps- og kontinuitetsplaner, oppdatering av behandlingsprotokoller og gjennomføring av øvelser på håndtering av alvorlige informasjonssikkerhets- eller personvernhendelser.

I tillegg ble det opplyst om at enkelte typer sikringstiltak, for eksempel innføring av totrinnsinnlogging, hadde blitt forsinket på grunn av pandemihåndteringen.

Den vanligste grunnen til at disse (og andre) aktiviteter ikke ble utført som planlagt, var behovet for å anvende ressursene til andre og viktigere oppgaver. Her dreide det seg om at medarbeidere som til vanlig jobbet med informasjonssikkerhet eller personvern ble satt inn i det krevende arbeidet med å sørge for at kjerneoppgaver fortsatt kunne utføres (administrasjon, undervisning, eksamen, osv.). Dermed måtte oppgaver på informasjonssikkerhets- og personvernområdet stilles i bero inntil videre.

## POSITIV EFFEKT

To institusjoner opplyste om at

korona-nedstengingen hadde hatt en positiv innvirkning på arbeidet med ledelsessystemer og internkontroll (GDPR). Disse institusjonene mente at nedstengingen særlig hadde bidratt til å tydeliggjøre behovet for økt satsning på informasjonssikkerhet og personvern.

Konsekvensen av dette var todelt. For det første at arbeidet med utvikling og innføring av ledelsessystemer og internkontroll (GDPR) fikk større fremdrift enn tidligere. For det andre at nye sikkerhets- og personverntiltak ble iverksatt eller at allerede planlagte tiltak ble hasteinnført.

Disse institusjonene la også vekt på at nedstengingen hadde ført økt bevissthet om informasjonssikkerhet og personvern.

## INGEN EFFEKT

Til sist var det fem institusjoner som opplyste om at korona-nedstengingen ikke hadde påvirket arbeidet med ledelsessystemer og internkontroll (GDPR) i vesentlig grad. Disse institusjonene mente derfor at arbeidet fortsatte som før nedstengingen – den hadde verken hatt en positiv eller negativ innvirkning.

## SAMLET VURDERING

Oppsummert kan vi si at håndtering av pandemien synes å ha medført at et flertall av universitetene og høgskolene fikk et etterslep i arbeidet med innføring og videreutvikling av et systematisk informasjonssikkerhets- og personvernarbeid.

Etterslepet vil måtte innhentes nå som situasjonen er i ferd med å normalisere seg.

# Ekstraordinære tiltak

## Pandemihåndteringen har altså ført til et visst etterslep i arbeidet med ledelsessystemer og internkontroll (GDPR) hos en del av universitetene og høgskolene.

Men «den nye normalen» med hjemmekontor, fjernundervisning og bruk av uvante kommunikasjons- og samhandlingsplattformer kan likevel ha gjort det nødvendig med ekstraordinære informasjonssikkerhets- eller personverntiltak. Dette er tiltak som enten ikke ville blitt iverksatt eller som ble iverksatt raskere enn opprinnelig tenkt på grunn av «den nye normalen».

Vi spurte derfor universitetene og høgskolene om de hadde innført ekstraordinære tiltak som en del av pandemihåndteringen.

Til sammen opplyste institusjonene om at det ble iverksatt 68 informasjonssikkerhets- og personverntiltak som følge av pandemihåndteringen.

Tre institusjoner rapporterte at de hadde iverksatt ett ekstraordinært tiltak hver. De fleste institusjonene (12) opplyste imidlertid om mellom to og fire tiltak. Fem institusjoner hadde iverksatt flere enn fire tiltak. Det høyeste antall tiltak som det ble opplyst om var åtte. Hvilke tiltak dette handlet om diskuteres nedenfor.

Kun én institusjon svarte at det ikke ble iverksatt ekstraordinære informasjonssikkerhets- eller personverntiltak.

Ut over dette ble det rapportert om en del tiltak som ikke handlet om informasjonssikkerhet og personvern. Det gjaldt for eksempel investeringer i AV-utstyr på undervisningsrom. Disse er ikke inkludert i oversikten nedenfor (figur 3) – den gir kun et bilde av tiltak som ble begrunnet (helt eller delvis) med hensynet til informasjonssikkerheten eller personvernet (eller begge deler).

### FLERCAMPUS-INSTITUSJONER

Enkelte flercampus-institusjoner, spesielt nylig omorganiserte institusjoner, mente at de ikke hadde behov for mange ekstraordinære tiltak.

Denne oppfatningen ble begrunnet med at «den nye normalen» var en del av institusjonenes etablerte orden: fjernarbeid, fjernundervisning og digital samhandling var ikke uvanlig også i tiden før pandemien. De mente derfor at det allerede var iverksatt mange tiltak for å motvirke den økte risikoen for uønskede hendelser som nedstengingen innebar. Behovet for ekstraordinære tiltak ble dermed mindre enn hva det ellers ville vært.

## KATEGORIER EKSTRAORDINÆRE TILTAK

De ekstraordinære tiltakene som institusjonene opplyste om, kan inndeles i fire kategorier:

**1) Tekniske tiltak:** anskaffelse av nye sikkerhetsløsninger eller oppgradering av teknisk utstyr for å styrke sikkerheten til informasjonsbehandlingen.

**2) Organisatoriske tiltak:** gjennomføring av visse typer sikkerhetsaktiviteter (risikovurderinger) eller innføring av nye rutiner eller retningslinjer for informasjonssikkerhet eller behandling av personopplysninger.

**3) Pedagogiske tiltak:** informasjon til brukerne om informasjonssikkerhet og personvern, for eksempel på hjemmekontor, og kurs/opplæring i sikker bruk av nye IT-løsninger.

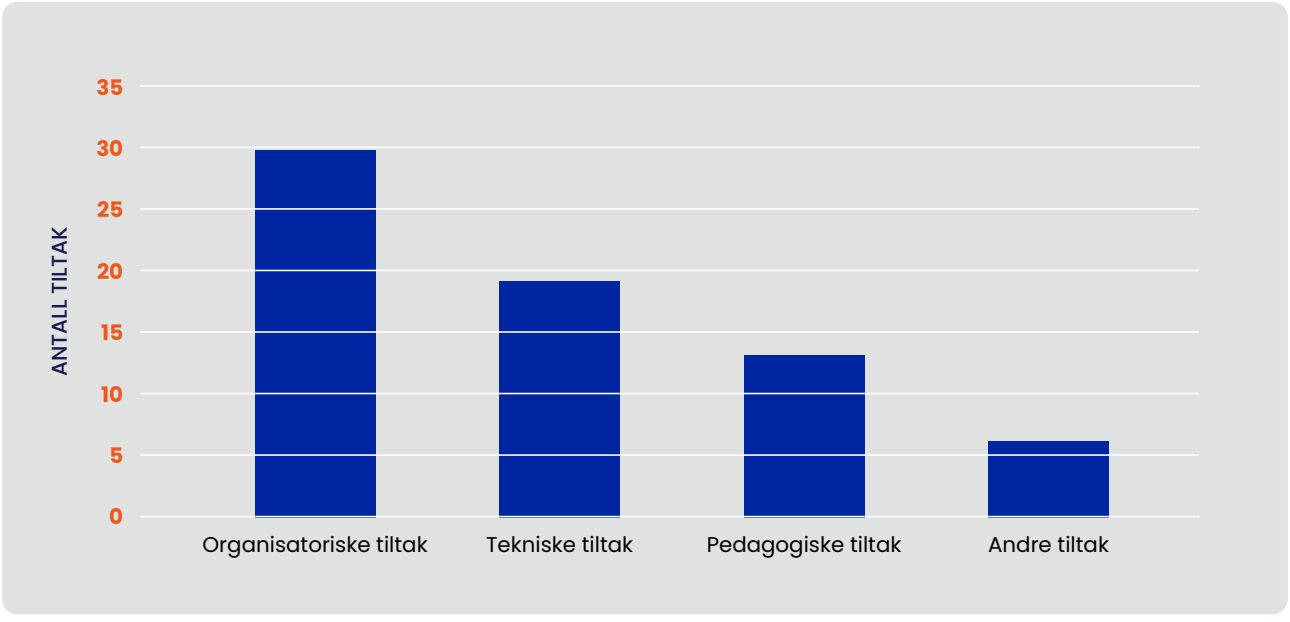
**4) Andre tiltak:** tiltak som ikke passer inn i de øvrige kategoriene, spesielt juridiske tiltak (samtykkeløsninger, inngåelse av databehandleravtaler med nye tjenesteleverandører, vurdering av behandlingsgrunnlag, osv.).

Figur 3 gir en oversikt over hvordan de 68 ekstraordinære tiltakene fordeler seg på de fire tiltakskategoriene.

Figuren viser at det ble rapportert om klart flest organisatoriske tiltak (30). Deretter følger tekniske (19) og pedagogiske tiltak (13).

I restkategorien «andre tiltak» finner vi noen relativt få tiltak (6). Som indikert ovenfor, gjelder de fleste av disse juridiske forhold.

Figur 3: Typer ekstraordinære tiltak



## ORGANISATORISKE TILTAK

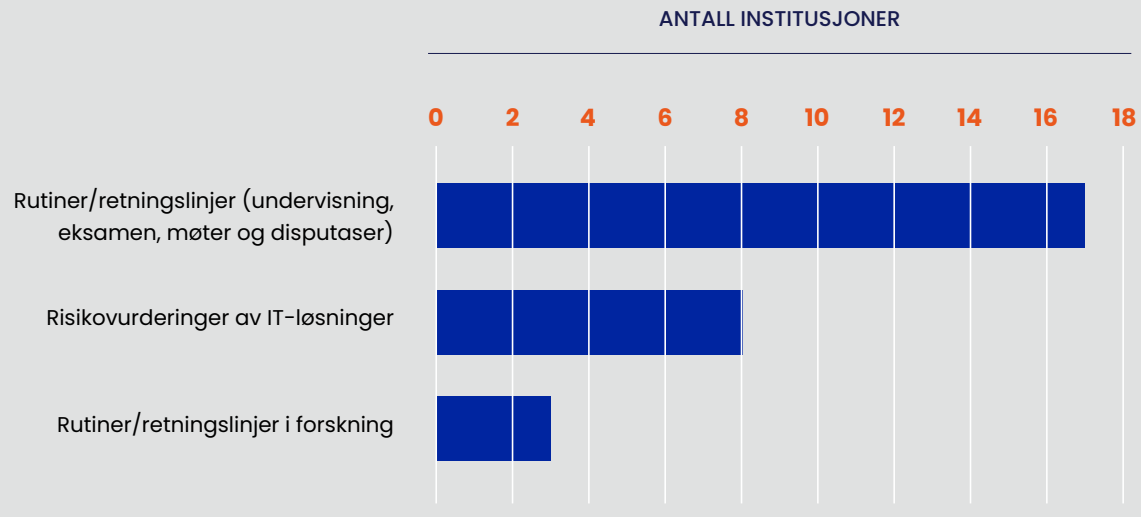
I figur 4 gis en oversikt over de vanligste ekstraordinære tiltakene av organisatorisk karakter som institusjonene rapporterte om.

Figuren viser at flest institusjoner (17) rapporterte om at det var utarbeidet nye rutiner eller retningslinjer for gjennomføring av kjerneoppgaver. Dette gjaldt spesielt digital undervisning, digital eksamen og digitale møter. Det var også flere institusjoner som opplyste om at det var laget tilsvarende rutiner eller retningslinjer for digitale disputaser.

Noen færre universiteter og høgskoler (8) opplyste om at det var gjennomført risikovurderinger av informasjonssikkerheten og personvernet i nye IT-løsninger, for eksempel Zoom og Teams. Hos disse institusjonene var det heller ikke uvanlig at digital eksamen og bruk av hjemmekontor ble risikovurdert.

Til sist opplyste enkelte institusjoner (3) om at det ble laget egne rutiner eller retningslinjer for sikker bruk av digitale kommunikasjonsløsninger. Det samme gjaldt for bruk av IT-utstyr i forskningsvirksomheten, spesielt ved innsamling av data (intervjuer).

Figur 4: Organisatoriske tiltak



## TEKNISKE TILTAK

Figur 5 viser hvilke ekstraordinære tekniske tiltak som det oftest ble rapportert om som følge av pandemihåndteringen.

Iverksatte tekniske tiltak fordeler seg nokså jevnt på de ulike hovedtypene i figuren.Ingen av de tekniske tiltakstypene peker seg derfor ut som vesentlig mer vanlige eller populære enn de andre.

Fire institusjoner rapporterte for eksempel om at det var iverksatt ekstraordinære tiltak for sikker elektronisk kommunikasjon – innføring av VPN, erstatte gammel VPN med eduVPN eller anskaffelse av flere VPN-lisenser. Det samme antallet institusjoner oppga at de hadde tatt i bruk løsninger for elektronisk signering av dokumenter.

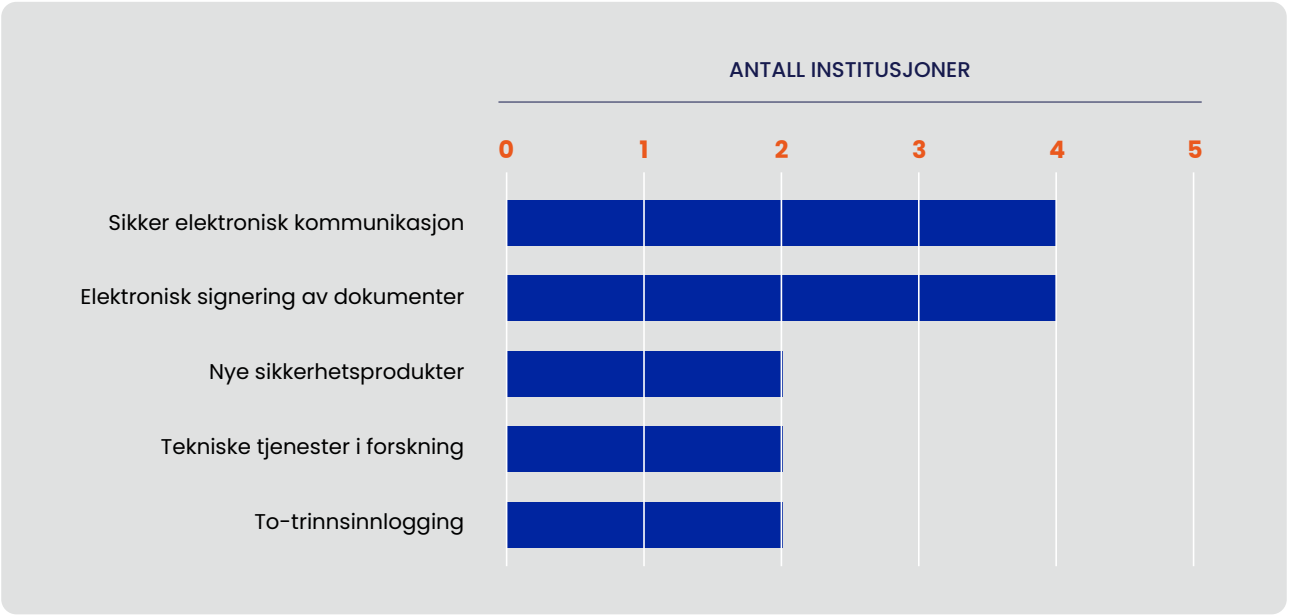
Like bak disse tiltakstypene følger bruk av nye sikkerhetsprodukter. Eksempler på dette er Cisco Umbrella og Microsoft Advanced Threat Protection. Deretter følger anskaffelse av tekniske tjenester for behandling av sensitive forskningsdata, spesielt Nettskjema/TSD levert av Universitetet i Oslo. Til slutt opplyste enkelte institusjoner om at det ble innført totrinnsinnlogging på VPN eller Office 365.

## PEDAGOGISKE TILTAK

Figur 6 gir en oversikt over de viktigste ekstraordinære tiltakene av pedagogisk art som universitetene og høgskolene svarte at de hadde iverksatt.

Det klart vanligste pedagogiske tiltaket var utarbeidelse og formidling av generell informasjon og gjennomføring av kurs (webinarer). Informasjonen og kursene fokuserte særlig på informasjonssikkerhet og personvern

Figur 5: Tekniske tiltak



på hjemmekontor. Ni universiteter og høgskoler opplyste om slike tiltak.

I tillegg opplyste to institusjoner om at det ble gitt særskilt informasjon om informasjonssikkerhet og personvern ved gjennomføring av digital eksamen.

Ytterligere to institusjoner rapporterte om at de enten hadde informert eller avholdt kurs om sikker bruk av nye IT-løsninger, spesielt Zoom og Teams.

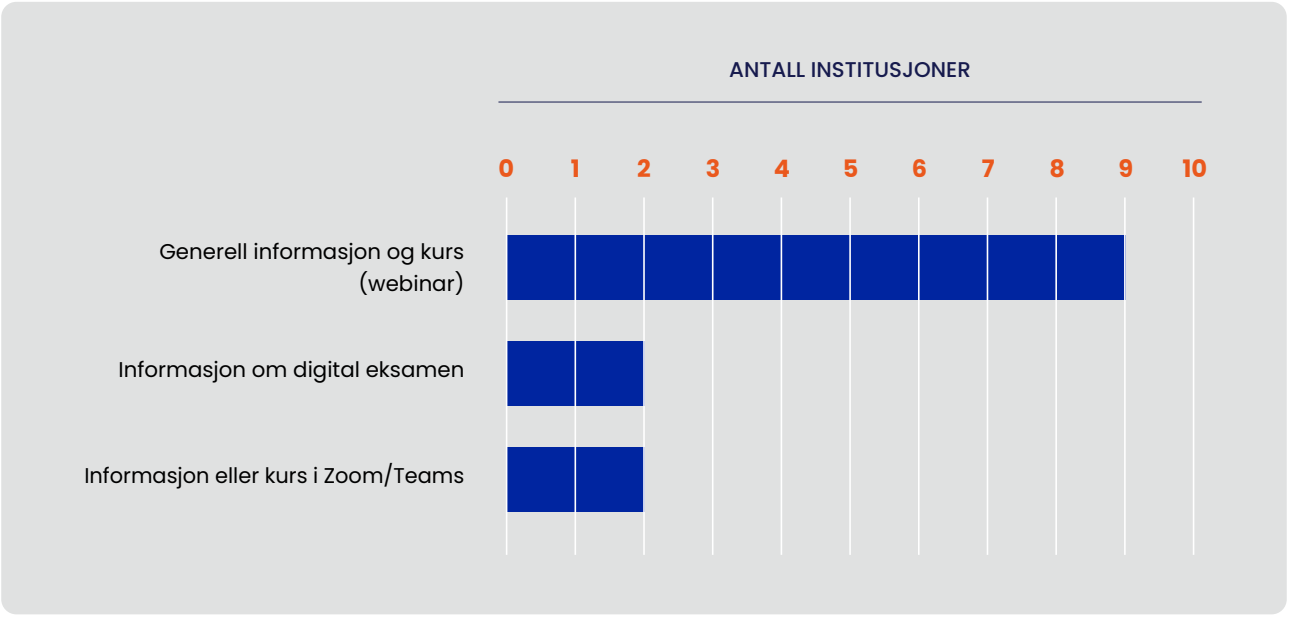
## TILTAKSAKTIVITET OG LANGSIKTIGHET

Pandemihåndteringen innebar at enkelte institusjoner omprioriterte ressurser til andre oppgaver enn innføring og videreutvikling av ledelsessystemer for informasjonssikkerhet og internkontrollen for personvern (GDPR). Universitetene og høgskolene hadde likevel iverksatt en rekke ekstraordinære informasjonssikkerhets- og personverntiltak. Tiltaksaktivitet i forbindelse med pandemihåndteringen har derfor ikke vært ubetydelig.

Mange av tiltakene, spesielt de organisatoriske og tekniske, vil trolig være viktige også etter at pandemien er over. Disse tiltakene er derfor ikke bare relevante i den aktuelle krisesituasjonen, men vil bidra til å styrke informasjonssikkerheten og personvernet også på lengre sikt.

Spørsmålet er likevel om de ekstraordinære tiltakene skissert ovenfor er tilstrekkelige sett i lys av de utfordringer som pandemien har ført med seg. Det er derfor viktig at ressurser prioriteres for å hente inn etterslepet som virker å ha oppstått i det systematiske arbeidet med ledelsessystemer og internkontroll (GDPR).

Figur 6: Pedagogiske tiltak



# Særskilte personvernutfordringer

## De ekstraordinære tiltakene hadde sin bakgrunn i nye utfordringer som pandemihåndteringen stilte universitetene og høgskolene ovenfor.

Vi var særlig opptatt av å fremskaffe informasjon om hvilke typer personvernutfordringer dette dreide seg om. Institusjonene ble derfor spurt om det hadde oppstått særskilte personvernutfordringer i forbindelse med korona-nedstengingen, og hvilke disse i så fall var.

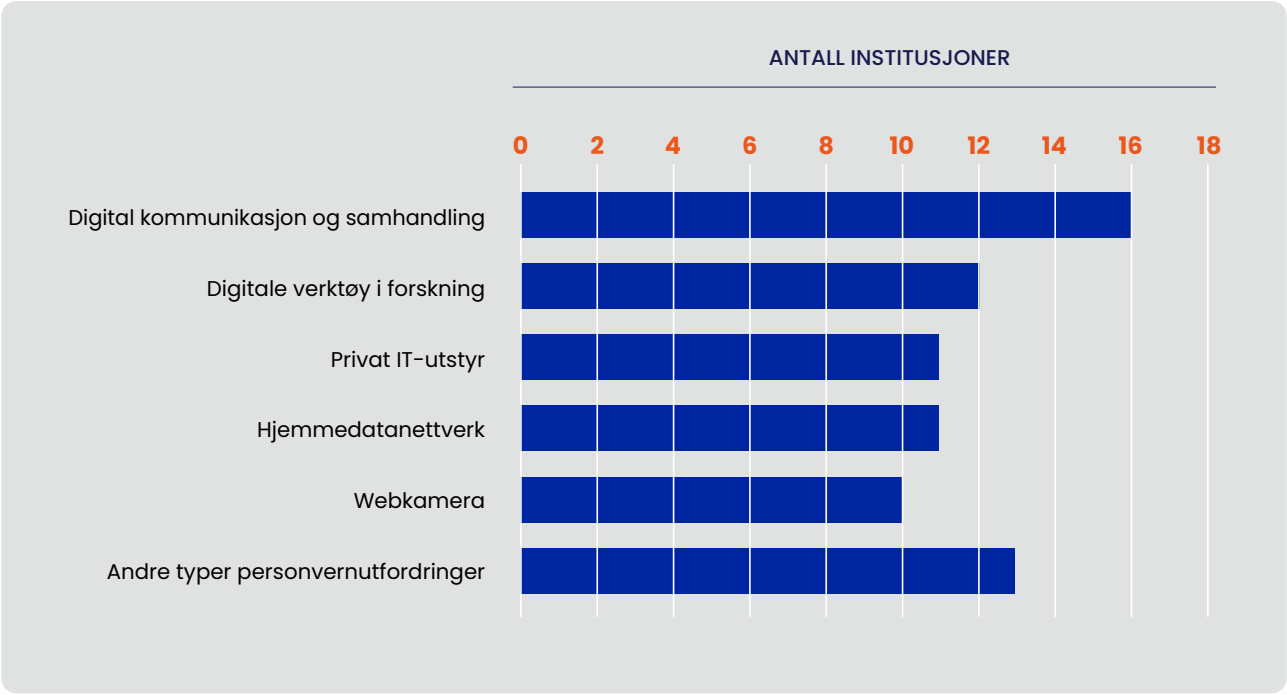
Figur 7 gir en oversikt over hva institusjonene svarte.

### DIGITAL KOMMUNIKASJON OG SAMHANDLING

Av figuren ser vi at problemstillinger knyttet til opptak og lagring av digital kommunikasjon og samhandling – digital undervisning, digital eksamen og disputaser, møter på Zoom og Teams, osv. – ble nevnt av flest institusjoner (16).

En særlig vanlig problemstilling i denne forbindelse var knyttet til rettslig grunnlag for den behandling av personopplysninger som skjer ved opptak av digital kommunikasjon og samhandling. Dette gjaldt for eksempel i tilfeller hvor lagring av undervisningsopptak var basert på samtykke for studenter og undervisere. Hvordan skulle institusjonene håndtere tilbaketrekking av samtykke og krav fra studenter eller undervisere om at opptakene ble slettet? Hva hvis andre studenter eller undervisere

**Figur 7: De vanligste personvernutfordringene**



ønsket at opptakene fortsatt skulle være tilgjengelige? Slike spørsmål hadde skapt en viss usikkerhet og diskusjon både blant studenter og ansatte, men hadde i de fleste tilfeller blitt håndtert ved at det ble utarbeidet egne retningslinjer for opptak og lagring.

I enkelte andre tilfeller hadde digitale løsninger blitt sperret mot lagring av opptak. Noen institusjoner hadde i tillegg laget særskilte retningslinjer for digital kommunikasjon og samhandling i visse typer studier. Dette gjaldt primært innen medisinske fag og fag som sykepleie, fysioterapi og psykologi.

## DIGITALE VERKTØY I FORSKNING

Bruk av digitale verktøy til innsamling og lagring av personopplysninger i forskning, var en annen problemstilling som ble nevnt av mange institusjoner (12). Her var det særlig sikkerheten ved behandling av personopplysninger som ble fremhevet som utfordrende. Dette gjaldt spesielt (men ikke bare) i prosjekter hvor det ble samlet inn særlige kategorier opplysninger om sårbare grupper, for eksempel i forbindelse med videoopptak av barn eller unge. Var tilgjengelige digitale verktøy og videokonferansetjenester (Zoom, Facetime, osv.) sikre nok til å kunne benyttes i slike sammenhenger?

Andre vanlige problemstillinger knyttet til digitale verktøy i forskning gjaldt sikkerheten ved bruk av private opptaksenheter – kunne privat IT-utstyr benyttes til opptak og lagring av intervjuer?

## PRIVAT IT-UTSTYR OG HJEMMEDATANETTVERK

De to neste kategoriene problemstillinger som ble nevnt av mange institusjoner, gjaldt også personopplysningssikkerhet. Disse handlet om (i) de ansattes bruk av privat IT-utstyr på hjemmekontor til behandling av personopplysninger og (ii) fjerntilgang til interne datasystemer over nettverk utenfor institusjonenes kontroll (hjemmedatanettverk). Institusjonene fordelte seg likt mellom disse to problemstillingene (nevnt av 11 institusjoner hver).

Når det gjaldt bruken av privat IT-utstyr, var bekymringene i første rekke knyttet til om utstyret var tilfredsstillende sikret mot uautorisert tilgang, spesielt dersom utstyret ble benyttet til lagring av opplysninger som institusjonene var rettslig ansvarlige for. Dette kunne føre til at institusjonene mistet kontrollen over opplysningene og at de kom på avveie. Noen institusjoner hadde håndtert denne risikoen ved å kjøpe inn bærbare datamaskiner til de ansatte.

Enkelte institusjoner opplyste også om sikkerhetsutfordringer ved bruk av jobb-maskiner på hjemmekontor. Det gjaldt blant annet hos institu-

sjoner som hadde opplevd at det var utfordrende å installere sikkerhetsoppdateringer på jobb-maskiner – oppdateringene ble blokkert i brannmuren til selskaper som leverer nettforbindelser til husstander.

Bruk av hjemmedatanettverk for tilgang til institusjonenes digitale systemer og tjenester reiste liknende utfordringer – institusjonene hadde liten innsikt i hvordan datanettverk var satt opp på hjemmekontor. De hadde derfor også begrenset kontroll med sikkerheten i datakommunikasjonen mellom hjemmekontor og institusjonenes datasystemer. Enkelte institusjoner opplyste for eksempel om utfordringer med å oppdage og stoppe skadevare og nettfiske-epost.

Mange av de tekniske tiltakene som er drøftet ovenfor tok sikte på å redusere risikoen for brudd på personopplysningssikkerheten ved bruk av hjemmedatanettverk. Eksempler på dette er innkjøp av nye VPN-lisenser, anskaffelse av eduVPN og innføring av totrinnsinnlogging ved fjernpålogging til institusjonenes IT-systemer eller -tjenester.

## WEBKAMERA

Den siste kategorien personvernutfordringer som mange institusjoner (10) svarte at de hadde vært opptatt av, var bruk av webkamera, spesielt i digital undervisning. Dette gjaldt i hvilken grad forelesere kunne kreve at studenter hadde kameraet på i undervisningssituasjoner, eller om personvernhensyn kunne begrunne at det var avslått, for eksempel for å skjerme mot innsyn i private hjem. Enkelte institusjoner opplyste om at tilsvarende problemstillinger hadde vært diskutert ved bruk av videokonferanseløsninger i forskning (intervjuer).

Også her hadde de fleste institusjonene håndtert utfordringene ved å utarbeide egne retningslinjer for bruk av webkamera. I tillegg ble det formidlet informasjon til studenter og ansatte om innholdet i retningslinjene.

## ANDRE PERSONVERN-UTFORDRINGER

Institusjonene opplyste også om en rekke andre utfordringer som ikke kan tilordnes kategoriene ovenfor. Disse omhandlet alt fra håndtering av utskrifter på hjemmekontor til registrering av oppmøte for smittesporingsformål. Andre utfordringer som ble nevnt handlet for eksempel om bruk av videokonferanseløsninger sett i lys av Schrems II-dommen (overføring av personopplysninger til USA) og diskusjoner om innføring av elektroniske løsninger for å avdekke eksamensfusk (ingen slike løsninger ble innført).

Institusjonene hadde valgt litt ulike tilnærminger til flere av utfordringene i «andre-kategorien». En fellesnevner er likevel at korona-nedstengingen ikke førte til bruk av løsninger for strengere elektronisk kontroll av arbeidshverdagen til studenter og ansatte.[14]

14 Undersøkelser fra andre land tyder på at jobbing fra hjemmekontor har ført til økt elektronisk overvåkning av de ansattes arbeidshverdag. Se for eksempel BBC, 05.11.2021: "The Way My Boss Monitored Me at Home is Creep" (https://www.bbc.com/news/uk-politics-59152864).

# Oppsummering – forsterket systematikk

**Korona-nedstenging, hjemmekontor og digital undervisning har ført til at universiteter og høgskoler er blitt mer avhengig av digitale løsninger for å utføre sine kjerneoppgaver. Det skyldes i første rekke økt og annerledes bruk av digitale systemer og tjenester snarere enn at mange nye er tatt i bruk.**

Sett i et informasjonssikkerhets- og personvernperspektiv, betyr økt avhengighet av digitale løsninger et større potensial for skade dersom løsningene ikke skulle virke som forutsatt. Det gjelder uavhengig av om årsaken er dataangrep, tekniske feil eller menneskelige uhell. Samtidig er det ikke usannsynlig at avhengigheten vil vare ved, for eksempel dersom hjemmearbeid og digital undervisning blir mer vanlig enn før pandemien.

I møte med pandemi-situasjonen har universitetene og høgskolene iverksatt en del ekstraordinære informasjons-sikkerhets- og personverntiltak. Tiltakene kan ha bidratt til at institu-sjonene ikke har opplevd vesentlig flere uønskede hendelser i perioder med korona-nedstenginger enn ellers. Unit/HK-dir sine årlige risiko- og til-standsvurderinger indikerer imidlertid at trusselbildet i sektoren er skjerpet. Dette, sammen med økt avhengighet av digitale løsninger, understreker betydningen av at universitetene og høgskolene (og øvrige virksom-heter i UH-sektoren) forsterker det systematiske arbeidet med informa-sjonssikkerhet og personvern.