|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Medarbejders adfærd ift. GDPR** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at 2 udvalgte medarbejdere interviewes med spørgsmål herunder (se ideer til konkrete spørgsmål på sidste side) | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Når medarbejdere behandler personoplysninger, skal de som en naturlig del af deres adfærd sikre, at personoplysninger ikke deles med uvedkommende og generelt håndteres korrekt | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Medarbejderen bekræfter, at mundtlig kommunikation med personoplysninger sker / er sket forsvarligt | |  |  |
| Medarbejderen bekræfter at lukke / låse til de lokaler som retningslinjer forskriver | |  |  |
| Medarbejderen bekræfter, ikke at kende andre medarbejderes login og adgangskoder | |  |  |
| Medarbejderen bekræfter at beskytte fortrolige og følsomme personoplysninger i daglige rutiner | |  |  |
| Medarbejderen bekræfter, at private enheder (fx mobiltelefon) ikke anvendes til institutionens aktiviteter | |  |  |
| Medarbejderen bekræfter at låse PC og mobile enheder, når de forlades | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Medarbejders viden om GDPR** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at 2 udvalgte medarbejdere skriftligt besvarer spørgsmål (fx ved at stille spørgsmål med flere svarmuligheder), der skal afdække deres viden om GDPR (se ideer til konkrete spørgsmål på sidste side) | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Når medarbejdere arbejder med personoplysninger, skal de have en forståelse for, at personoplysninger skal behandles med omtanke og efter reglerne | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| At medarbejdere har en tilstrækkelig viden om hvordan personoplysninger håndteres korrekt.  Fx at der kun må indsamles personoplysninger, der er relevante for at løse opgaven, og at mundtlig kommunikation skal ske under hensyn til at evt. uvedkommendes kan lytte med | |  |  |
| At medarbejdere har en nødvendig viden om at omfanget af data bør minimeres  Fx at der kun sker opbevaring af personoplysninger, hvis det har et formål og at det er nødvendigt løbende at slette personoplysninger | |  |  |
| At medarbejderen kender kontaktpersoner, hvis der er spørgsmål til GDPR-forhold herunder spørgsmål fra de registrerede borgere mv. | |  |  |
| At medarbejderen kan identificere persondatabrud / sikkerhedsbrud | |  |  |
| At medarbejderen kender den person der skal kontaktes ved persondatabrud | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Fysiske forhold i institutionens lokaler** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at lave en fysisk gennemgang af lokaler herunder de fysiske forhold fx adgangsmuligheder, låse, skabe mv. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Behandling af personoplysninger skal ske med tilstrækkelige fysiske foranstaltninger, der sikrer en god beskyttelse af personoplysninger | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| At det kun er relevante personoplysninger, der er synlige på institutionens fællesarealer (fx på opslagstavler, whiteboards mv.) og at informationerne som udgangspunkt kun er tilgængelige for dem det vedrører | |  |  |
| Tag 2 stikprøver på, at medarbejdere ikke opbevarer brugernavn og adgangskode skriftligt fx på fysisk papir, eller er noteret på en måde / på et medie hvor informationerne kan være tilgængelige for andre | |  |  |
| Det kontrolleres, at opbevaringen af personoplysninger med særlig fokus på at fortrolige og følsomme af personoplysninger sker jf. institutionens retningslinjer – fx opbevaring i skabe, at kontorer er låst, at skriveborde er ryddet, at mapper med personoplysninger er opbevaret sikkert og/eller er skærmet for uvedkommende | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Personoplysninger på fysiske dokumenter** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at lave en gennemgang af fysiske dokumenter / noter mv., uanset hvor de befinder sig, og uanset hvad baggrunden er for, at de findes. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Personoplysninger (og særligt fortrolige og følsomme personoplysninger), der findes på fysiske dokumenter / noter mv. skal beskyttes, så de ikke kommer til uvedkommendes kendskab | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver på, at midlertidigt registrerede personoplysninger på fysiske dokumenter (fx på telefonnotater, referater, løse noter, dokumenter til arkivering eller lignende) er opbevaret sikkert | |  |  |
| Tag 2 stikprøver på, at der ikke forefindes fysiske dokumenter (fx notater, referater, løse noter, dokumenter til arkivering eller lignende) med personoplysninger, der burde være registreret i fagsystemer | |  |  |
| Tag 2 stikprøver på, at der ikke forefindes fysiske dokumenter (fx notater, referater, løse noter, dokumenter til arkivering eller lignende) med personoplysninger der burde være slettet/tilintetgjort jf. fastlagte sletteregler | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Personoplysninger i systemer / enheder** | **Gennemføres uge X** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at gennemgå indholdet af personoplysninger i it- / fagsystemer og it-enheder | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Personoplysninger bør registreres og håndteres i it-systemer med den bedste databeskyttelse i forhold til typen af oplysning.  Personoplysninger skal slettes fra it-systemer og it-enheder, når der ikke er et lovligt formål med at opbevare oplysningerne længere | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver af, at der ikke registreres flere personoplysninger end det er nødvendigt for at institutionen kan løfte sine bundne opgaver, dvs. oplysninger der ikke har relevans for opgaveløsningen. | |  |  |
| Tag 2 stikprøver af, at der ikke er opbevaret personoplysninger (fx i borger- eller medarbejdersager) i længere tid end der er et lovligt formål hermed (jf. fastlagt slettefrister) | |  |  |
| Tag 2 stikprøver af, at nye og gamle billeder kun opbevares / er slettet som anført i institutionens retningslinjer | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Billeder og kommunikation med borger** | **Gennemføres uge** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at gennemgå de enkelte kommunikationsområder, og undersøge hvorvidt interne retningslinjer for kommunikation med personoplysninger er overholdt | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  Samtykke skal være overholdt, og den skriftlige kommunikation med personoplysninger skal ske på en sikker måde og kun med rette vedkommende | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Find de evt. personer hvor der **ikke** er givet samtykke til offentliggørelse af billeder på (fx sociale medier, hjemmesider mv) og kontroller, at der ikke findes billeder af disse personer | |  |  |
| Det kontrolleres, at personer på offentliggjorte billeder (uanset hvor de er offentliggjort) ikke burde føle sig krænket | |  |  |
| Tag 2 stikprøver af mails og kontroller, at de overholder institutionens regler for kommunikation via mail. (fx hvis der er en regel om, at der ikke må være omfattet fortrolige og følsomme oplysninger i mailen) | |  |  |
| Tag 2 stikprøver af mails med personoplysninger og kontroller, at de er sendt til korrekt modtager | |  |  |
| Det kontrolleres, at evt. skriftlig kommunikation (ml. borger og institution) gennem andet end via mail ikke indeholder personoplysninger. Det kunne fx være gennem SMS | |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| KONTROLPLAN | | RESULTAT AF KONTROL | |
| **Borgers/medarbejderes (registreret) rettigheder** | **Gennemføres uge** | **Forbedringer / tiltag** | **Tidsfrist** |
| **Håndtering:**  Kontrollen gennemføres ved at spørge relevante personer og eller undersøge registreringer / gemte mailbesvarelser. | | [Anfør i punktform tiltag der skal gennemføres] |  |
| **Reglen er:**  At borgere og medarbejdere (registrerede) skal grundlæggende være oplyst om indhold og omfang af de behandlinger, der fortages af institutionen (oplysningspligt). Desuden skal de registrerede have besvaret løbende spørgsmål til institutionens behandling af den registreredes oplysninger. | |
| **Følgende kontroller gennemføres** | | **Beskrivelse af fremgangsmåde, observationer og resultat af kontrol** | **Kontroldato** |
| Tag 2 stikprøver af, at medarbejdere har modtaget privatlivspolitik ved ansættelsen fx ved at spørge medarbejderen om de har set politikken. | |  |  |
| Tag 2 stikprøver på, at borgere har modtaget privatlivspolitik ved ankomst til institutionen fx ved at spørger borgeren om de har set politikken. | |  |  |
| Tag 2 stikprøver på at borgeres henvendelser om ændringer til egne personoplysninger har medført korrekte ændringer i institutionens registreringer (fx adresseændring, personlige oplysninger etc) | |  |  |
| Undersøg om borgere har henvendt sig med spørgsmål til egne oplysninger og undersøg om henvender har modtaget svar - fx ved at undersøge mailbesvarelse eller spørge henvender. | |  |  |

**IDEER TIL SPØRGSMÅL I FORBINDELSE MED KONTROL AF MEDARBEJDER ADFÆRD OG VIDEN**

|  |  |
| --- | --- |
| **EMNE - ADFÆRD** | **IDEER TIL SPØRGSMÅL** |
| Medarbejderen bekræfter, at mundtlige kommunikation med personoplysninger sker / er sket forsvarligt | Hvis du skal tale med en kollega fx om den daglige håndtering af en borger, tager du så nogle særlige hensyn for samtalen? |
| Medarbejderen bekræfter at lukke / låse til de lokaler som retningslinjer forskriver | Hvilke døre skal være lukket eller låst her hos os?  Gør du det? |
| Medarbejderen bekræfter, ikke at kende andre medarbejderes login og adgangskoder | Kender du dine kollegaers adgangskoder?  Når du skal logge ind i [fagsystem], hvordan gør du så? |
| Medarbejderen bekræfter at beskytte fortrolige og følsomme personoplysninger i daglige rutiner | Hvordan beskytter du fortrolige eller følsomme oplysninger i dagligdagen? |
| Medarbejderen bekræfter, at private enheder (fx mobiltelefon) ikke anvendes til institutionens aktiviteter | Bruge du din mobiltelefon på arbejdet … og til hvad? |
| Medarbejderen bekræfter at låser PC og mobile enheder, når de forlades | Hvordan beskytter du adgangen til vores PC-er, iPads mv. når du ikke bruger disse? |
| **EMNE - VIDEN** | **IDEER TIL SPØRGSMÅL – (**spørgsmål med flere svarmuligheder) |
| At medarbejdere generelt har en tilstrækkelig viden om korrekt håndtering af personoplysninger | Hvad er korrekt håndtering af personoplysninger  Oplysninger indsamles for at løse en driftsopgave (korrekt)  Oplysninger gemmes fordi de er rare at have, hvis de måske skal bruges igen (ikke korrekt)  Samme oplysninger opbevares på papir og i system for en sikkerheds skyld (ikke korrekt)  Oplysninger kan uden problemer sendes til anden institution (Ikke korrekt)  Kommunikation med personoplysninger skal ske uden at uvedkommende kan følge med (korrekt) |
| At medarbejdere har en nødvendig viden om betydning af dataminimering | Hvad betyder det at dataminimerer:  At der indsamledes så mange personoplysninger som muligt for at være sikker (ikke korrekt)  At personoplysning kun opbevares hvis det er et krav (korrekt)  At dokumenter / sager med personoplysninger løbende skal slettes (korrekt)  At det er nødvendigt at gemme alle billeder der er taget (ikke korrekt) |
| At medarbejderen kender kontaktpersoner, hvis der er spørgsmål til GDPR-forhold herunder spørgsmål fra de registrerede borgere mv. | Hvem i institutionen skal du kontakte, hvis en borger har spørgsmål til de personoplysninger, som i har om vedkommende? |
| At medarbejderen kan identificere persondatabrud / sikkerhedsbrud | Giv 3 eksempler på hændelser, der muligvis kan anses som et databrud eller et sikkerhedsbrud? |
| At medarbejderen kender den person, der skal kontaktes ved persondatabrud | Hvem i institutionen skal du kontakte, hvis du har opdaget noget, der kunne være et databrud eller et sikkerhedsbrud? |