

## Privatliv, sikkerhed og tryghed i det digitale energilandskab



|  |   |
|--|---|
| Privatliv, sikkerhed og tryghed i det digitale energilandskab..... | 1 |
| Sådan fungerer dette kursus .....                                  | 2 |
| Læringsmål .....   | 2 |
| Introduktion .....   | 3 |
| Digitale teknologier og den digitale energiomstilling.....         | 3 |
| Cybersikkerhed i energisektoren.....                               | 4 |
| Forbedring af din energiprivatliv, sikkerhed og tryghed .....      | 5 |
| Konklusion .....   | 6 |
| Yderligere ressourcer .....  | 6 |
| Tak.....   | 7 |
| Billedkreditering.....   | 7 |

## Sådan fungerer dette kursus

Dette korte kursus på 30 minutter forklarer, hvad privatliv, sikkerhed og tryghed betyder i forbindelse med digitalisering af energisektoren. Kurset behandler også bekymringer om brugen af intelligente energiteknologier.

Du er måske interesseret i at:

- Være interesseret i at bruge smarte teknologier til at få et bedre overblik over dit energiforbrug, men usikker på, hvordan du beskytter dine personlige oplysninger.
- Være nysgerrig efter at vide, hvordan dine personlige oplysninger bruges og deles, når du bruger digitale teknologier.
- Ønske at få en bedre forståelse af privatliv, sikkerhed og tryghed i forbindelse med digitalisering af energi.

Dette kursus vil give dig en dybere forståelse af den digitale energiomstilling og støtte din egen digitale energirejse! Det er en del af en serie på 12 kurser kaldet [Digital Energy Essentials](#) (Væsentlige elementer i digital energi), der er udviklet af Every1-projektet, som har til formål at gøre det muligt for alle at engagere sig i energiomstillingen. Du kan finde ud af mere om projektet på: <https://every1.energy>

Ved afslutningen af kurset foreslår vi nogle yderligere læringsmaterialer, som du kan udforske. Dette omfatter kurset [What is the Digital Energy Transition? \(Hvad er den digitale energiomstilling?\)](#), som undersøger, hvad digital energi er, og årsagerne til at gå i retning af digitalisering af vores produktion og forbrug af energi.

Dette er en oversættelse af den originale [engelske version af kurset](#), som giver mulighed for at gennemføre en kort quiz og opnå et Every1-digitalt badge.

Dette projekt har modtaget finansiering fra Den Europæiske Unions Horizon-program for forskning og innovation (2021-2027) under tilskudsaf tale nr. 101075596. Det fulde ansvar for indholdet af dette kursus ligger hos Every1-projektet og afspejler ikke nødvendigvis Den Europæiske Unions holdning.

## Læringsmål

Efter at have gennemgået dette korte kursus bør du være i stand til at:

- Skelne mellem privatliv, sikkerhed og tryghed i forbindelse med digitalisering af energi.
- Forstå de største udfordringer i forbindelse med at sikre privatliv, sikkerhed og tryghed, når man bruger digitale teknologier til energi.
- Være opmærksom på dine rettigheder i henhold til den generelle forordning om databeskyttelse (GDPR) i relation til energidata.

- Anvende praktiske råd til at beskytte dine data og forbedre din digitale energisikkerhed.

## Introduktion



I takt med at digitale teknologier bliver en integreret del af vores liv, bliver privatliv, sikkerhed og beskyttelse af vores personlige oplysninger i forbindelse med digitalisering af energiområdet stadig vigtigere.

Intelligente målere, mobile apps og andre digitale enheder indsamler og deler data for at forbedre energieffektiviteten, men dette kan også give

anledning til bekymringer om databeskyttelse og sikkerhed.

Før vi går i gang, skal vi se nærmere på, hvad vi mener med databeskyttelse, sikkerhed og tryghed. Dette er indbyrdes forbundne, men forskellige begreber:

- **Privatlivets fred** vedrører beskyttelsen af personlige oplysninger.
- **Tryghed** indebærer at sikre, at brugen af digitale teknologier ikke medfører fysisk eller psykisk skade.
- **Sikkerhed** fokuserer på at beskytte data mod uautoriseret adgang eller angreb.

I dette kursus vil vi ikke kun se på forskellige udfordringer for vores energiprivatliv, sikkerhed og beskyttelse, men også på handlinger, du kan foretage for at beskytte dig selv. Vi vil også se på, hvordan regeringer og energileverandører beskytter dig og dine data, samt den infrastruktur, der muliggør brugen af digitale teknologier til energiproduktion og -forbrug.

## Digitale teknologier og den digitale energiomstilling

Som du måske har set i kurset [Smarte enheder og digital energiteknologi](#), der udforsker forskellige typer smarte enheder mere indgående, findes der en række digitale teknologier, der understøtter digitaliseringen af energi.

Det digitale energilandskab er et komplekst økosystem af sammenkoblede teknologier og interesser. Nøglekomponenterne omfatter:

- **Smartmålere:** Enheder, der automatisk indsamler og overfører data om energiforbrug til energileverandører. Smartmålere giver mere nøjagtig fakturering, indsigt i forbrugsmønstre og mulighed for at deltage i efterspørgselsresponsprogrammer, hvor du kan justere dit energiforbrug på baggrund af efterspørgsels- og prissignaler.
- **Smarte elnet:** Moderniserede elnet, der bruger digitale teknologier til at overvåge og styre strømmen af elektricitet. De muliggør tovejskommunikation mellem

forsyningselskabet og forbrugeren, hvilket giver mulighed for overvågning af energiforbruget i realtid og integration af vedvarende energikilder.

- **Tingenes internet (IoT) inden for energi:** Netværk af forbundne enheder (termostater, apparater, EV-opladere), der indsamler og udveksler data, hvilket muliggør fjernstyring og optimering af energiforbruget.

Data om energi kan omfatte forbrugsmønstre, data om brugstid, detaljer på apparatniveau og endda adfærdsdata, der kan udledes af brugen. Disse data kan hjælpe dig med at forstå dit eget energiforbrug, potentielt spare penge og træffe informerede valg. De kan også hjælpe energileverandører (f.eks. din elleverandør) med at optimere elnettet, tilbyde dig personaliserede tjenester og opdage svindel.

Dine energidata indsamles typisk af din energileverandør, men de kan også deles med eller tilgås af måleroperatører, dataaggregatorer, tredjepartsudbydere og potentielt offentlige myndigheder. Energidata er nyttige for politiske beslutningstagere, f.eks. ved at understøtte udviklingen af effektive energipolitikker og -regler.



Data om energiforbrug kan indeholde følsomme oplysninger. Da en række forskellige organisationer kan have adgang til dine data og bruge dem på forskellige måder, kan dette give anledning til bekymring. Senere i kurset vil vi foreslå nogle måder, hvorpå du kan forbedre din energiprivatliv, sikkerhed og tryghed. Lad os først se på nogle almindelige cybertrusler og hvad der gøres for at sikre sikkerheden i digitale systemer.

### Cybersikkerhed i energisektoren

Den digitale transformation af energisektoren har gjort den til et mål for cyberangreb, som kan forstyrre energiforsyningen og kompromittere følsomme oplysninger. Almindelige cybertrusler omfatter:

- **Malware** (ondsindet software, der kan skade computersystemer og data).
- **Ransomware** (en type ondsindet software, der krypterer dine filer, gør dem utilgængelige og kræver en løsesum for at genoprette adgangen).
- **Denial-of-service-angreb** (disse angreb har til formål at overbelaste et system eller netværk med trafik, så det bliver utilgængeligt for legitime brugere).
- **Phishing-svindel** (svigagtige forsøg på at få fat i følsomme oplysninger, såsom adgangskoder eller kreditkortoplysninger, ved at udgive sig for at være en troværdig enhed).

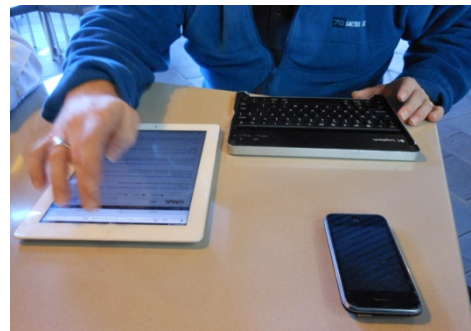
Beskyttelse af kritisk infrastruktur kræver foranstaltninger som netværkssegmentering, hvilket er praksis med at opdele et større netværk i mindre, isolerede segmenter. Dette

begrænser spredningen af cyberangreb og inddæmmer potentiel skade, begrænser adgangen til kontrolfunktioner, opdager og forhindrer indtrængende og muliggør tilpasset adgang til kontrolfunktioner.

[EU's cybersikkerhedslov](#) styrker cybersikkerheden i hele EU og fastsætter regler for certificering af sikkerheden af produkter og tjenester. Det er afgørende at sikre sikkerheden af digitale energisystemer. Dette omfatter:

- **Cyberfysiske systemer:** Beskyttelse af disse systemer, hvor fysisk infrastruktur styres digitalt, mod cyberangreb, der kan have konsekvenser i den virkelige verden.
- **Sikkerhedsstandarder:** Overholdelse af EU's sikkerhedsstandarder for digitale enheder og energisystemer for at sikre deres sikre brug og vedligeholdelse.

Den [generelle forordning om databeskyttelse \(GDPR\)](#) giver dig specifikke [rettigheder](#) vedrørende dine personoplysninger, herunder energidata. Disse rettigheder vedrørende dine personoplysninger omfatter:



- **Ret til adgang:** Du kan anmode om en kopi af dine energidata fra din udbyder.
- **Retten til berigtigelse:** Du kan anmode om, at eventuelle unøjagtige eller manglende data korrigeres eller opdateres.
- **Ret til sletning:** Du kan anmode om sletning af dine data under visse omstændigheder.
- **Ret til begrænsning af behandling:** Du kan begrænse, hvordan dine data bruges.
- **Ret til dataportabilitet:** Du kan modtage dine data i et overførbart format.

### Forbedring af din energiprivatliv, sikkerhed og tryghed

Da digitalisering af energi og brugen af digitale teknologier til at styre vores forbrug og produktion af energi bliver mere og mere almindeligt, er her et par tips, der kan hjælpe dig med at forbedre din energiprivatliv, sikkerhed og tryghed.

- **Sikr dine smarte enheder:** Brug stærke adgangskoder, aktiver tofaktorautentificering, og hold softwaren opdateret.
- **Beskyt dit netværk:** Sikkerhedstil dit Wi-Fi-netværk, undgå offentlige Wi-Fi-netværk til følsomme aktiviteter, og overvej at bruge en firewall.
- **Kontroller dine data:** Gennemgå privatlivspolitikkerne omhyggeligt, udøv dine GDPR-rettigheder, og fravælg datadeling, hvis du ikke er komfortabel med det.

Det digitale energilandskab er i konstant udvikling, og der dukker regelmæssigt nye teknologier og trusler op. Det er vigtigt at holde sig informeret om disse tendenser for at sikre dit privatliv, sikkerhed og tryghed.

Her er nogle eksempler på nye teknologier, der spiller eller i fremtiden kan komme til at spille en mere central rolle i digitaliseringen af energi:

- **Blockchain-teknologi:** Blockchain, en decentraliseret regnskabsteknologi, har potentiale til at revolutionere energidatastyring ved at tilbyde en sikker, gennemsigtig og manipulationssikker måde at spore og dele data på.
- **Kunstig intelligens (AI) og maskinlæring (ML):** AI- og ML-algoritmer kan bruges til at analysere energidata, opdage afvigelser og forudsige potentielle sikkerhedstrusler, hvilket forbedrer den samlede sikkerhed i energisystemer.
- **Kvantecomputere:** Selvom kvantecomputere stadig er i deres barndom, har de potentiale til at forstyrre eksisterende krypteringsmetoder, hvilket udgør en ny udfordring for datasikkerheden i energisektoren.



## Konklusion

Den digitale transformation af energisektoren rummer enorme muligheder for et mere bæredygtigt, effektivt og kundecentreret energisystem. Fordelene ved denne overgang kan dog kun realiseres fuldt ud, hvis vi aktivt og kontinuerligt tager fat på udfordringerne med energiprivatliv, sikkerhed og tryghed.

Som energiforbrugere har vi en vigtig rolle at spille i udformningen af en sikker digital energifremtid. Ved at forstå vores rettigheder i henhold til GDPR, tage proaktive skridt til at beskytte vores data og vælge energileverandører og tjenesteudbydere, der prioriterer privatlivets fred og sikkerhed, kan vi sikre, at vores personlige oplysninger forbliver beskyttede. Desuden kan vi ved at holde os informeret om cybersikkerhedstrusler og bedste praksis bidrage til at beskytte den energiinfrastruktur, som vi alle er afhængige af.

Overgangen til et digitalt energisystem handler ikke kun om teknologi, men også om at give enkeltpersoner og samfund mulighed for aktivt at deltage i den digitale energiomstilling. Ved at omfavne digitale værktøjer og træffe informerede valg kan vi bidrage til en renere, mere pålidelig og mere retfærdig energifremtid.

## Yderligere ressourcer

- Læs mere om dine rettigheder i henhold til EU's databeskyttelsesregler i *Hvad er mine rettigheder?* [https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights\\_en#:~:text=object%20to%20the%20processing%20of,controller%20\('data%20portability'\)%3B](https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en#:~:text=object%20to%20the%20processing%20of,controller%20('data%20portability')%3B)
- Få mere at vide om EU's cybersikkerhedslov og hvordan den beskytter dig <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

- Se en konsekvensanalyse vedrørende databeskyttelse (DPIA) for intelligente elnet og intelligente målere. [https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment\\_en](https://energy.ec.europa.eu/topics/markets-and-consumers/smart-grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en)
- Læs mere om, hvordan Europa-Kommissionen beskytter os, i denne artikel om *kritisk infrastruktur og cybersikkerhed*. [https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity\\_en](https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en)

## Tak

*Privatliv, sikkerhed og tryghed i det digitale energilandskab* er en bearbejdelse af udvalgte tekster fra Det Internationale Energiagenturs (IEA) "Data Privacy in the Digital Energy Era" <https://www.iea.org/reports/digitalisation-and-energy> og "Enhancing cyber resilience in electricity systems" <https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems>, (de "originale værker"), som begge er licenseret under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/). Denne bearbejdning er udarbejdet og offentliggjort af Every1-projektet ("bearbejderen") og licenseret under [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/), medmindre andet er angivet. Dette er et værk, der er afledt af IEA-materiale af Every1-projektet, og Every1-projektet er alene ansvarligt for dette afledte værk. Det afledte værk er på ingen måde godkendt af IEA.

Adapteren har ændret de originale værker på følgende punkter:

- Tilpasningen fokuserer specifikt på aspekterne energi, privatliv, sikkerhed og sikkerhed i de originale værker.
- Det tekniske sprog er blevet forenklet for et bredt publikum.
- Der er tilføjet praktiske tips.
- Der er indarbejdet nye oplysninger fra kilder i Europa-Kommissionen for at dække GDPR og EU's cybersikkerhedslov.

## Billedkreditering

Hovedkursusbillede: [Untitled](#) af Mike Fritcher er licenseret [CC BY-SA 2.0](https://creativecommons.org/licenses/by-sa/2.0/).

Introduktion: [Kvinde, der bruger Windows Mobile-enhed i park med barn](#) af Gail er licenseret [CC BY-ND 2.0](https://creativecommons.org/licenses/by-nd/2.0/).

Digitale teknologier og den digitale energiomstilling: [Smart meter "Echelon"](#) af Patrik Tschudin er licenseret [under CC BY 2.0](https://creativecommons.org/licenses/by/2.0/).

Cybersikkerhed i energisektoren: [Mobil arbejdstager](#) af Michael Coghlan er licenseret [under CC BY-SA 2.0](https://creativecommons.org/licenses/by-sa/2.0/).

Forbedring af din energiprivatliv, sikkerhed og tryghed: [data](#) af Arismendy Polanco deles på en [Public Domain Mark 1.0](https://creativecommons.org/licenses/publicdomain/1.0/).