

## Privātums, drošība un aizsardzība digitālajā enerģētikas vidē



|   |   |
|---|---|
| Privātums, drošība un aizsardzība digitālajā enerģētikas vidē ..... | 1 |
| Kā darbojas šis kurss.....  | 2 |
| Mācību rezultāti .....  | 2 |
| Ievads .....  | 3 |
| Digitālās tehnoloģijas un digitālā enerģētikas pāreja .....         | 3 |
| Kiberdrošība enerģētikas nozarē.....                                | 4 |
| Jūsu enerģijas privātuma, drošības un aizsardzības uzlabošana ..... | 5 |
| Secinājums.....   | 6 |
| Papildu resursi.....  | 6 |
| Pateicības .....  | 7 |
| Attēlu avoti.....   | 7 |

## Kā darbojas šis kurss

Šis īss, 30 minūšu garš kurss izskaidro, ko nozīmē privātums, drošība un aizsardzība enerģētikas digitalizācijas kontekstā. Kursā tiek aplūkotas arī bažas par viedo enerģētikas tehnoloģiju izmantošanu.

Jūs varētu būt:

- Interesējaties par viedo tehnoloģiju izmantošanu, lai labāk izprastu savu enerģijas patēriņu, bet neesat pārliecināts, kā nodrošināt savu personas datu drošību.
- Jūs interesē, kā jūsu personas dati tiek izmantoti un kopīgoti, lietojot digitālās tehnoloģijas.
- Vēlaties labāk izprast privātumu, drošību un aizsardzību enerģētikas digitalizācijas kontekstā.

Šis kurss padziļinās jūsu izpratni par digitālo enerģētikas pāreju un atbalstīs jūsu paša digitālo enerģētikas ceļojumu! Tas ir daļa no 12 kursu kopuma ar nosaukumu „[Digital Energy Essentials](#)” (Digitālās enerģētikas pamati), ko izstrādājis projekts „Every1”, kura mērķis ir veicināt un nodrošināt ikviena iesaistīšanos enerģētikas pārejā. Vairāk informācijas par projektu varat atrast šeit: <https://every1.energy>

Kursu beigās mēs ieteiksim jums papildu mācību materiālus, ar kuriem varat iepazīties. Tas ietver kursu „[Kas ir digitālā enerģētikas pāreja?](#)”, kurā tiek izpētīts, kas ir digitālā enerģētika un kādi ir izejas, kāpēc mēs virzāmies uz enerģijas ražošanas un patēriņa digitalizāciju.

Šis ir [kurša](#) oriģinālās [angļu valodas versijas](#) tulkojums, kas ietver iespēju aizpildīt īsu testu un iegūt Every1 digitālo nozīmīti.

Šis projekts ir saņēmis finansējumu no Eiropas Savienības pētniecības un inovāciju programmas „Apvārsnis” (2021–2027) saskaņā ar dotāciju līgumu Nr. 101075596. Par šī kursa saturu atbildīgs ir tikai Every1 projekts, un tas ne vienmēr atspoguļo Eiropas Savienības viedokli.

## Mācību rezultāti

Pēc šī īsā kursa apguves jums vajadzētu būt spējīgiem:

- Atšķirt privātumu, drošību un aizsardzību enerģijas digitalizācijā.
- Saprast galvenās problēmas privātuma, drošības un aizsardzības nodrošināšanā, izmantojot digitālās tehnoloģijas enerģētikā.
- Apzināties savas tiesības saskaņā ar Vispārīgo datu aizsardzības regulu (GDPR) saistībā ar enerģētikas datiem.
- Piemērot praktiskus padomus, lai aizsargātu savus datus un uzlabotu savu digitālo enerģētikas drošību.

## levads



Tā kā digitālās tehnoloģijas kļūst par neatņemamu mūsu dzīves sastāvdaļu, privātums, drošība un aizsardzība saistībā ar mūsu personisko informāciju enerģētikas digitalizācijas kontekstā kļūst arvien svarīgāka.

Viedie skaitītāji, mobilās lietotnes un citas digitālās ierīces vāc un dalās ar datiem, lai uzlabotu energoefektivitāti, bet tas var radīt bažas par datu

privātumu un drošību.

Pirms sākam, aplūkosim sīkāk, ko mēs saprotam ar datu privātumu, drošību un aizsardzību. Šie jēdzieni ir savstarpēji saistīti, bet atšķirīgi:

- **Privātums** attiecas uz personas datu aizsardzību.
- **Drošība** nozīmē nodrošināt, ka digitālo tehnoloģiju izmantošana nerada fizisku vai psiholoģisku kaitējumu.
- **Drošība** ir vērsta uz datu aizsardzību pret neatļautu piekļuvi vai uzbrukumiem.

Šajā kursā mēs ne tikai apskatīsim dažādus izaicinājumus saistībā ar mūsu enerģētikas privātumu, drošību un aizsardzību, bet arī pasākumus, ko jūs varat veikt, lai sevi aizsargātu. Mēs arī apskatīsim, kā valdības un enerģijas piegādātāji aizsargā jūs un jūsu datus, kā arī infrastruktūru, kas ļauj izmantot digitālās tehnoloģijas enerģijas ražošanai un patēriņam.

## Digitālās tehnoloģijas un digitālā enerģētikas pāreja

Kā jūs varbūt esat redzējuši kursā „[Viedās ierīces un digitālās enerģētikas tehnoloģijas](#)”, kurā tiek padziļināti izpētīti dažādi viedo ierīču veidi, pastāv virkne digitālo tehnoloģiju, kas atbalsta enerģētikas digitalizāciju.

Digitālā enerģētikas vide ir sarežģīta savstarpēji saistītu tehnoloģiju un ieinteresēto pušu ekosistēma. Galvenās sastāvdaļas ir šādas:

- **Viedie skaitītāji:** ierīces, kas automātiski vāc un nosūta datus par enerģijas patēriņu enerģijas piegādātājiem. Viedie skaitītāji nodrošina precīzāku rēķinu izrakstīšanu, ieskatu patēriņa modeļos un iespēju piedalīties pieprasījuma reaģēšanas programmās, kurās varat pielāgot enerģijas patēriņu atbilstoši pieprasījumam un cenu signāliem.
- **Viedie tīkli:** modernizēti elektrotīkli, kas izmanto digitālās tehnoloģijas, lai uzraudzītu un kontrolētu elektrības plūsmu. Tie nodrošina divvirzienu komunikāciju starp komunālo pakalpojumu sniedzēju un patērētāju, ļaujot reāllaikā uzraudzīt enerģijas patēriņu un integrēt atjaunojamās enerģijas avotus.

- **Lietu internets (IoT) enerģētikā:** savienotu ierīču (termostati, sadzīves tehnika, elektromobiļu uzlādētāji) tīkls, kas vāc un apmainās ar datiem, ļaujot attālināti kontrolēt un optimizēt enerģijas patēriņu.

Dati par enerģiju var ietvert patēriņa modeļus, lietošanas laika datus, informāciju par sadzīves tehniku un pat uzvedības datus, kas iegūti no lietošanas. Šie dati var palīdzēt jums izprast savu enerģijas patēriņu, iespējams, ietaupīt naudu un pieņemt apzinātus lēmumus. Tie var palīdzēt arī enerģijas piegādātājiem (piemēram, jūsu elektroenerģijas piegādātājam) optimizēt tīklu, piedāvāt jums personalizētus pakalpojumus un atklāt krāpšanu.

Jūsu enerģijas datus parasti vāc jūsu enerģijas piegādātājs, bet tos var arī koplietot ar skaitītāju operatori, datu apkopotājiem, trešo pušu pakalpojumu sniedzējiem un, iespējams, valsts iestādēm, vai arī tie var piekļūt šiem datiem. Enerģijas dati ir noderīgi politikas veidotājiem, piemēram, atbalstot efektīvas enerģētikas politikas un regulējuma izstrādi.



Dati par enerģijas patēriņu var ietvert konfidenciālu informāciju. Tā kā dažādas organizācijas var piekļūt jūsu datiem un izmantot tos dažādos veidos, tas var radīt bažas. Kursā vēlāk ieteiksim dažus veidus, kā uzlabot enerģijas privātumu, drošību un aizsardzību. Vispirms apskatīsim dažas izplatītas kiberdraudības un to, kas tiek darīts, lai nodrošinātu digitālo sistēmu drošību.

### Kiberdrošība enerģētikas nozarē

Enerģētikas nozares digitālā transformācija ir padarījusi to par mērķi kiberuzbrukumiem, kas var traucēt enerģijas piegādi un apdraudēt konfidenciālu informāciju. Bieži sastopami kiberdraudi ir:

- **Ļaunprogrammatūras** (ļauņprātīgas programmatūras, kas var kaitēt datoru sistēmām un datiem).
- **Izspiešanas programmatūra** (ļauņprātīga programmatūra, kas šifrē jūsu failus, padarot tos nepieejamus, un pieprasa izpirkuma maksu, lai atjaunotu piekļuvi).
- **Pakalpojumu atteikuma uzbrukumi** (šo uzbrukumu mērķis ir pārslodzēt sistēmu vai tīklu ar datu plūsmu, padarot to nepieejamu likumīgiem lietotājiem).
- **Pishinga krāpšanas** (krāpnieciski mēģinājumi iegūt konfidenciālu informāciju, piemēram, paroles vai kredītkartes datus, izliekoties par uzticamu organizāciju).

Kritiskās infrastruktūras aizsardzībai nepieciešami tādi pasākumi kā tīkla segmentācija, kas ir prakse, kurā lielāku tīklu sadala mazākos, izolētos segmentos. Tas ierobežo kiberuzbrukumu

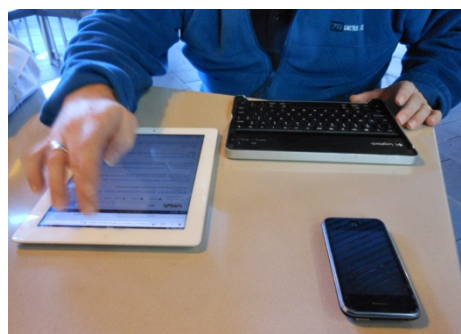
izplatību un ierobežo potenciālos zaudējumus, ierobežo piekļuvi kontroles mehānismiem, atklāj un novērš ieburcējus un nodrošina pielāgotu piekļuvi kontroles mehānismiem.

[ES kiberdrošības akts](#) uzlabo kiberdrošību visā ES un nosaka noteikumus produktu un pakalpojumu drošības sertificēšanai. Digitālo enerģētikas sistēmu drošības nodrošināšana ir ļoti svarīga. Tas ietver:

- **Kiberfiziskās sistēmas:** šo sistēmu, kurās fiziskā infrastruktūra tiek pārvaldīta digitāli, aizsardzība pret kiberuzbrukumiem, kas var radīt reālas sekas.
- **Drošības standartus:** ES drošības standartu ievērošanu digitālajām ierīcēm un enerģētikas sistēmām, lai nodrošinātu to drošu lietošanu un uzturēšanu.

[Vispārīgā datu aizsardzības regula \(GDPR\)](#) piešķir jums konkrētas [tiesības](#) saistībā ar jūsu personas datiem, tostarp enerģijas datiem. Šīs tiesības saistībā ar jūsu personas datiem ietver:

- **Piekļuves tiesības:** jūs varat pieprasīt kopiju saviem enerģijas datiem no sava pakalpojuma sniedzēja.
- **Tiesības uz labošanu:** jūs varat pieprasīt, lai jebkādi neprecīzi vai trūkstoši dati tiktu laboti vai atjaunināti.
- **Tiesības uz dzēšanu:** Jūs varat pieprasīt savu datu dzēšanu noteiktos apstākļos.
- **Tiesības ierobežot apstrādi:** jūs varat ierobežot savu datu izmantošanu.
- **Tiesības uz datu pārnesamību:** jūs varat saņemt savus datus pārnesamā formātā.



### Jūsu enerģijas privātuma, drošības un aizsardzības uzlabošana

Tā kā enerģētikas digitalizācija un digitālo tehnoloģiju izmantošana enerģijas patēriņa un ražošanas pārvaldībā kļūst par ikdienu, šeit ir daži padomi, kas palīdzēs jums uzlabot enerģētikas privātumu, drošību un aizsardzību.

- **Aizsargājiet savas viedierīces:** izmantojiet drošas paroles, aktivizējiet divpakāpju autentifikāciju un regulāri atjauniniet programmatūru.
- **Aizsargājiet savu tīklu:** aizsargājiet savu Wi-Fi tīklu, izvairieties no publiskā Wi-Fi izmantošanas jutīgām darbībām un apsveriet iespēju izmantot ugunsūri.
- **Kontrolējiet savus datus:** rūpīgi pārskatiet privātuma politiku, izmantojiet savas GDPR tiesības un atteikties no datu koplietošanas, ja jums tas nepatīk.

Digitālā enerģētikas vide nepārtraukti attīstās, regulāri parādoties jaunām tehnoloģijām un draudiem. Lai nodrošinātu savu privātumu, drošību un aizsardzību, ir svarīgi būt informētam par šīm tendencēm.

Šeit ir daži piemēri jaunām tehnoloģijām, kuras jau tagad vai nākotnē varētu spēlēt nozīmīgāku lomu enerģētikas digitalizācijā:

- **Blokķēdes tehnoloģija:** Blokķēde, decentralizēta grāmatvedības tehnoloģija, var radīt revolūciju enerģētikas datu pārvaldībā, nodrošinot drošu, pārredzamu un neaizskaramu veidu, kā izsekot un dalīties ar datiem.
- **Mākslīgais intelekts (AI) un mašīnmācīšanās (ML):** AI un ML algoritmus var izmantot, lai analizētu enerģētikas datus, atklātu anomālijas un prognozētu potenciālos drošības draudus, uzlabojot enerģētikas sistēmu kopējo drošību.
- **Kvantu skaitļošana:** lai gan kvantu skaitļošana vēl atrodas sākuma stadijā, tai ir potenciāls izjaukt esošās šifrēšanas metodes, radot jaunu izaicinājumu datu drošībai enerģētikas nozarē.



## Secinājums

Enerģētikas nozares digitālā transformācija piedāvā milzīgas iespējas izveidot ilgtspējīgāku, efektīvāku un uz klientu orientētu enerģētikas sistēmu. Tomēr šīs pārejas priekšrocības var pilnībā realizēt tikai tad, ja mēs aktīvi un nepārtraukti risinām enerģētikas privātuma, drošības un aizsardzības problēmas.

Kā enerģijas patērētājiem mums ir būtiska loma drošas digitālās enerģētikas nākotnes veidošanā. Izprotot savas tiesības saskaņā ar GDPR, veicot proaktīvus pasākumus, lai aizsargātu savus datus, un izvēloties enerģijas piegādātājus un pakalpojumu sniedzējus, kuri prioritāri pievēršas privātumam un drošībai, mēs varam nodrošināt, ka mūsu personas informācija paliek aizsargāta. Turklāt, pastāvīgi sekojot līdzi kibernetikas draudumiem un labākajai praksei, mēs varam palīdzēt aizsargāt enerģētikas infrastruktūru, uz kuru mēs visi paļaujamies.

Pāreja uz digitālo enerģētikas sistēmu nav saistīta tikai ar tehnoloģijām, bet arī ar indivīdu un kopienu pilnvarošanu aktīvi piedalīties digitālajā enerģētikas pārejā. Izmantojot digitālos rīkus un pieņemot apzinātas izvēles, mēs varam veicināt tīrāku, uzticamāku un taisnīgāku enerģētikas nākotni.

## Papildu resursi

- Lasiet vairāk par savām tiesībām saskaņā ar ES datu aizsardzības noteikumiem sadaļā „Kādas ir manas tiesības?” [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)
- Uzziniet vairāk par ES kibernetikas aktu un to, kā tas jūs aizsargā <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- Iepazīstieties ar datu aizsardzības ietekmes novērtējumu (DPIA) viedo tīklu un viedo skaitītāju jomā. <https://energy.ec.europa.eu/topics/markets-and-consumers/smart->

[grids-and-meters/data-protection-impact-assessment-smart-grid-and-smart-metering-environment\\_en](#)

- Uzziniet vairāk par to, kā Eiropas Komisija mūs aizsargā, lasot šo rakstu par *kritisko infrastruktūru un kiberdrošību*. [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)

## Pateicības

*Privātums, drošība un aizsardzība digitālajā enerģētikas vidē* ir atlasītu materiālu adaptācija no Starptautiskās enerģētikas aģentūras (IEA) publikācijām „Datu privātums digitālajā enerģētikas ērā” <https://www.iea.org/reports/digitalisation-and-energy> un „Kiberizturības uzlabošana elektroenerģijas sistēmās” <https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems> (turpmāk „oriģinālās publikācijas”), kurām abām ir piešķirta [CC BY 4.0](#) licence. Šo adaptāciju ir veicis un publicējis Every1 projekts (turpmāk „adaptētājs”) un tā ir licencēta saskaņā ar [CC BY 4.0](#), ja vien nav norādīts citādi. Šis ir darbs, ko Every1 projekts ir izveidojis, balstoties uz IEA materiālu, un Every1 projekts ir vienīgais atbildīgais par šo atvasināto darbu. Atvasinātais darbs nekādā veidā nav apstiprināts no IEA puses.

Adapteris modificēja oriģinālos darbus šādos aspektos:

- Adaptācija īpaši koncentrējas uz oriģinālās versijas enerģētikas privātuma, drošības un aizsardzības aspektiem.
- Tehniskā valoda ir vienkāršota, lai būtu saprotama plašākai auditorijai.
- Ir pievienoti praktiski padomi.
- Ir iekļauta jauna informācija no Eiropas Komisijas avotiem, lai aptvertu VDAR un ES kiberdrošības aktu.

## Attēlu avoti

Galvenais kursa attēls: [Untitled](#), autors Mike Fritcher, licence [CC BY-SA 2.0](#).

Ievads: [Sieviete, kas parkā ar bērnu lieto Windows Mobile ierīci](#), autors Gail, licence [CC BY-ND 2.0](#).

Digitālās tehnoloģijas un digitālā enerģētikas pāreja: [viedais skaitītājs „Echelon”](#) (autors Patrik Tschudin) ir licencēts [CC BY 2.0](#).

Kiberdrošība enerģētikas nozarē: [Mobilais darbinieks](#), autors Michael Coghlan, licence [CC BY-SA 2.0](#).

Jūsu enerģētikas privātuma, drošības un aizsardzības uzlabošana: [dati](#), autors Arismendy Polanco, ir kopīgojams saskaņā ar [Public Domain Mark 1.0](#).