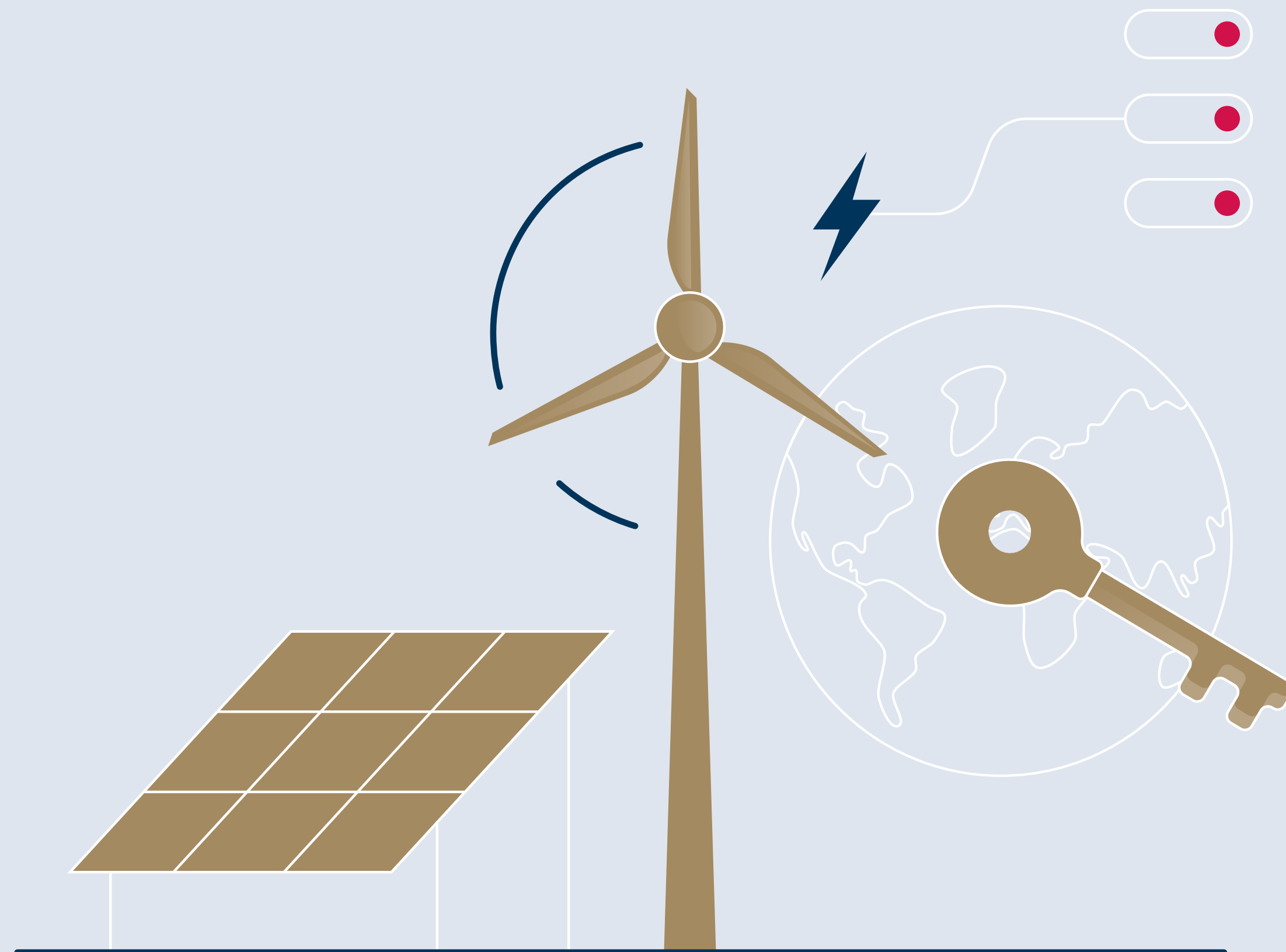


Beskyt dansk energiteknologi og innovation



Dansk landbrugs- drone sætter nye standarder for præcision



– og afdækker alle kabler i Østersøen

Som en del af det energiteknologiske forskningsmiljø på universiteterne eller i industrien har du ikke kun ansvaret for din faglige integritet, men også for at sikre, at viden og indsigt fra det energiteknologiske forskningsmiljø ikke bliver udnyttet i sammenhænge, der strider mod Danmarks sikkerhedsinteresser.

PET anbefaler, at du aktivt forholder dig til og overvejer mulige risici i dine samarbejdsaftaler, ansættelser og projekter – både nationale og internationale. Du bør derfor være opmærksom på, bl.a. hvem du samarbejder med, hvilke data og informationer du deler, og hvem der finansierer dine projekter eller investerer i din virksomhed.

Truslen mod

bioteknologi i Danmark

Dansk forskning og udvikling i energiteknologier er internationalt anerkendt, og energiteknologi vil fremover få meget stor betydning for dansk forsyningssikkerhed og økonomi. Derfor er du med dit arbejde en del af et af Danmarks vigtigste, men også mest udsatte forsknings- og udviklingsområder.

Din forskning kan være et muligt mål for både spionage og uønsket vidensoverførsel fra ikke-ligesindede stater, der ønsker at erhverve sig den nyeste viden inden for det energiteknologiske område. Hvis dit arbejde ender i de forkerte hænder, risikerer du uforvarende at bidrage til en styrkelse af ikke-ligesindede staters militære kapaciteter.

Dual-use/dobbelt anvendelse:

Produkter, software, teknologi og viden, der kan anvendes til både civile og militære formål.



Fremmede staters interesse

Både Kina og Rusland er villige til at bruge deres dominerende positioner inden for råstoffer og kritiske mineraler som sikkerhedspolitisk pression. Men begge lande agerer også mere offensivt i Danmark. De kinesiske efterretningstjenester forsøger fx til stadighed at indhente oplysninger om dansk teknologi og forskning på det energiteknologiske område.

Desuden er det PET's vurdering, at der udgår en sabotagetrussel fra den russiske stat mod især energi- og transportsektorerne, og som faciliteres af en forudgående spionageindsats. Spionagen er rettet mod vigtige oplysninger om fx it-systemer, teknisk udstyr, samarbejdspartnere og medarbejdere med relation til Danmarks kritiske infrastruktur. Også her er der derfor en betydelig trussel for uønsket vidensoverførsel.

Kontakt og ressourcer:

www.pet.dk/sikkerinnovation



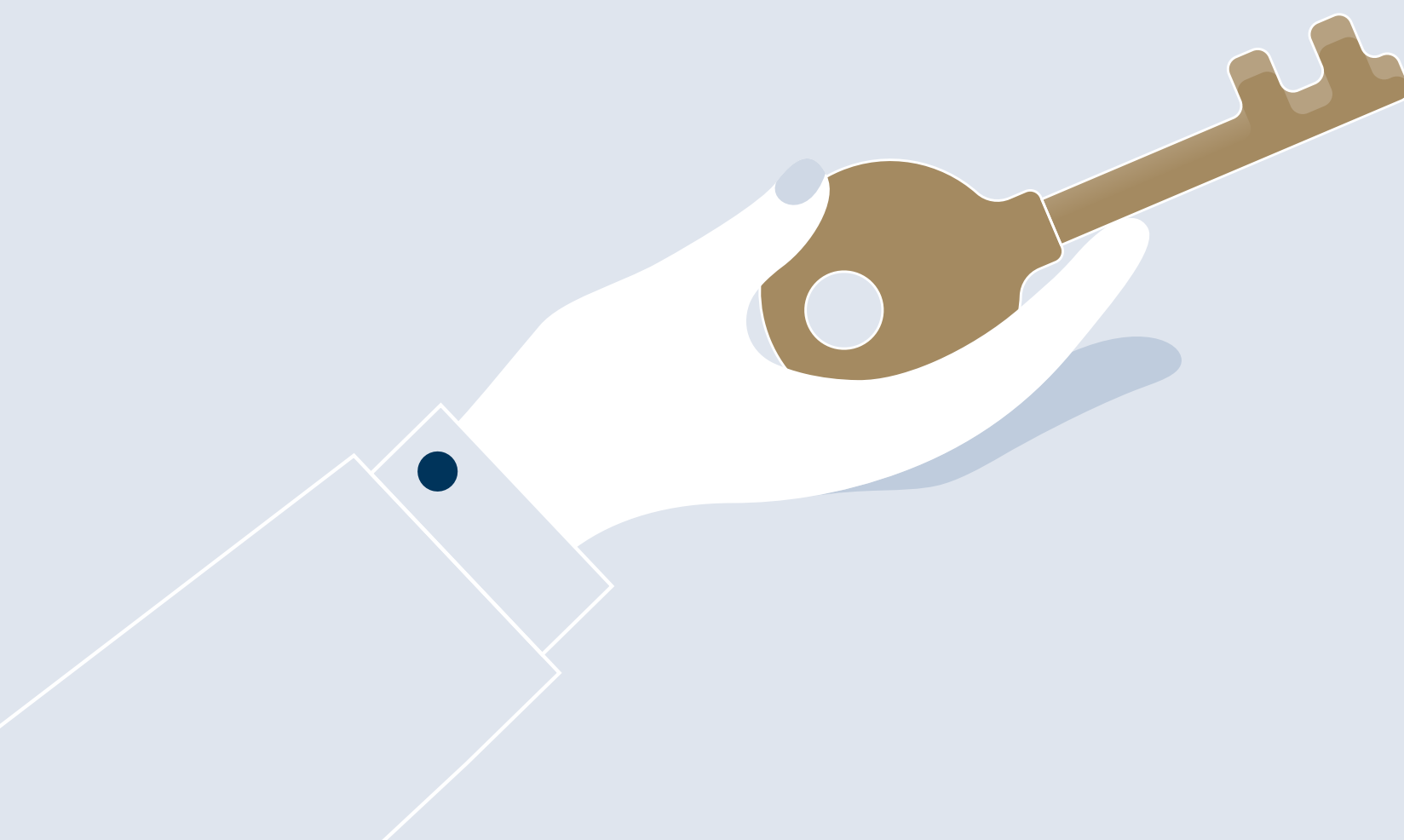
Ulovlig vidensoverførsel er i strid med fx spionage- eller eksportregler, mens **uønsket vidensoverførsel** finder sted, når teknologien ikke er kontrolleret, men kan stride mod Danmarks strategiske interesser. Uønsket vidensoverførsel sker bl.a. i forbindelse med grundforskning på det energiteknologiske område.

Civilt og militært potentiale

PET vurderer, at energiteknologier som eksempelvis lagrings- og konverteringsteknologier samt modulære atomare teknologier har et stort potentiale både civilt og militært. Truslen mod det energiteknologiske område retter sig dog ikke kun mod den specifikke udvikling af energiteknologi, men også mod teknologier, der er forudsætningsskabende for Danmarks energiforsyning og kritiske infrastruktur. Det gælder fx halvledere, kabler og batterilagringssystemer.

Hvad kan du gøre?

For at vurdere, om det er risikoen værd at lukke andre ind i dit forskningsmiljø, anbefaler PET, at du gør dig en række overvejelser, inden du fx vælger en ny leverandør, takker ja til en ny investering eller påbegynder et nyt samarbejde.



Overvej følgende, før du indgår et samarbejde

- 01 Det, du er god til, kan være det, andre gerne vil have fat i**

Overvej, hvorfor din forskning eller din virksomhed er særlig interessant i andres øjne. Du skal passe godt på det, du er særligt god til.

 - Står det helt klart for dig, hvem der står bag interessen for dit arbejde?
 - Er der noget helt særligt at vinde for dig ved et eventuelt samarbejde?
- 02 Dit arbejde kan have strategisk, militær eller politisk værdi**

Overvej mulighederne for misbrug af dit arbejde. Selvom dit arbejde retter sig mod civil brug, kan det have potentiale for militær anvendelse særligt for ikke-likesindede stater som Kina og Rusland, der også gerne vil være førende på det energiteknologiske område globalt.

 - Kan teknologien også anvendes i militær sammenhæng eller til overvågningsformål?
 - Behandler du i dit arbejde følsomme data, fx om sundhed, befolkning eller infrastruktur?

03 Forstå, hvem du reelt samarbejder med

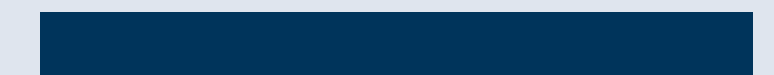
Overvej, hvor meget du ved om nye samarbejdspartnere. Det er vigtigt, at du kender deres baggrund – også de dele, de ikke selv fortæller dig om. Dybere viden om dine eventuelle samarbejdspartneres baggrund ruster dig til bedre at kunne vurdere, om de fx har forbindelse til ikke-likesindede staters militær eller uønskede civile aktører.

- Stemmer de opgivne publikationer eller samarbejder overens med, hvad du kan finde online?
- Har samarbejdspartneren tilknytning til militære institutioner, eller har denne haft det på et tidligere tidspunkt?
- Har samarbejdspartneren forbindelser til aktører i risikolande eller på sanktionslister?

04 Digitale, faglige og fysiske adgangsveje til dit arbejde

Overvej, hvad et samarbejde giver andre adgang til hos jer. Tænk over, hvad du potentielt giver andre adgang til – ikke kun fysisk, men også digitalt og fagligt, så en samarbejdspartner ikke får indsigt i strategier, planer eller idéer, som du ikke ønsker at dele.

- Vil din samarbejdspartner få adgang til fysiske faciliteter, som afslører vigtige detaljer om jeres forskning eller produktion?
- Vil du skulle give andre adgang til jeres vigtigste data, produkter eller nye idéer?
- Vil du i samarbejdet give adgang til kritisk infrastruktur eller store datasæt med følsomme oplysninger?



Kontakt og ressourcer:
www.pet.dk/sikkerinnovation

