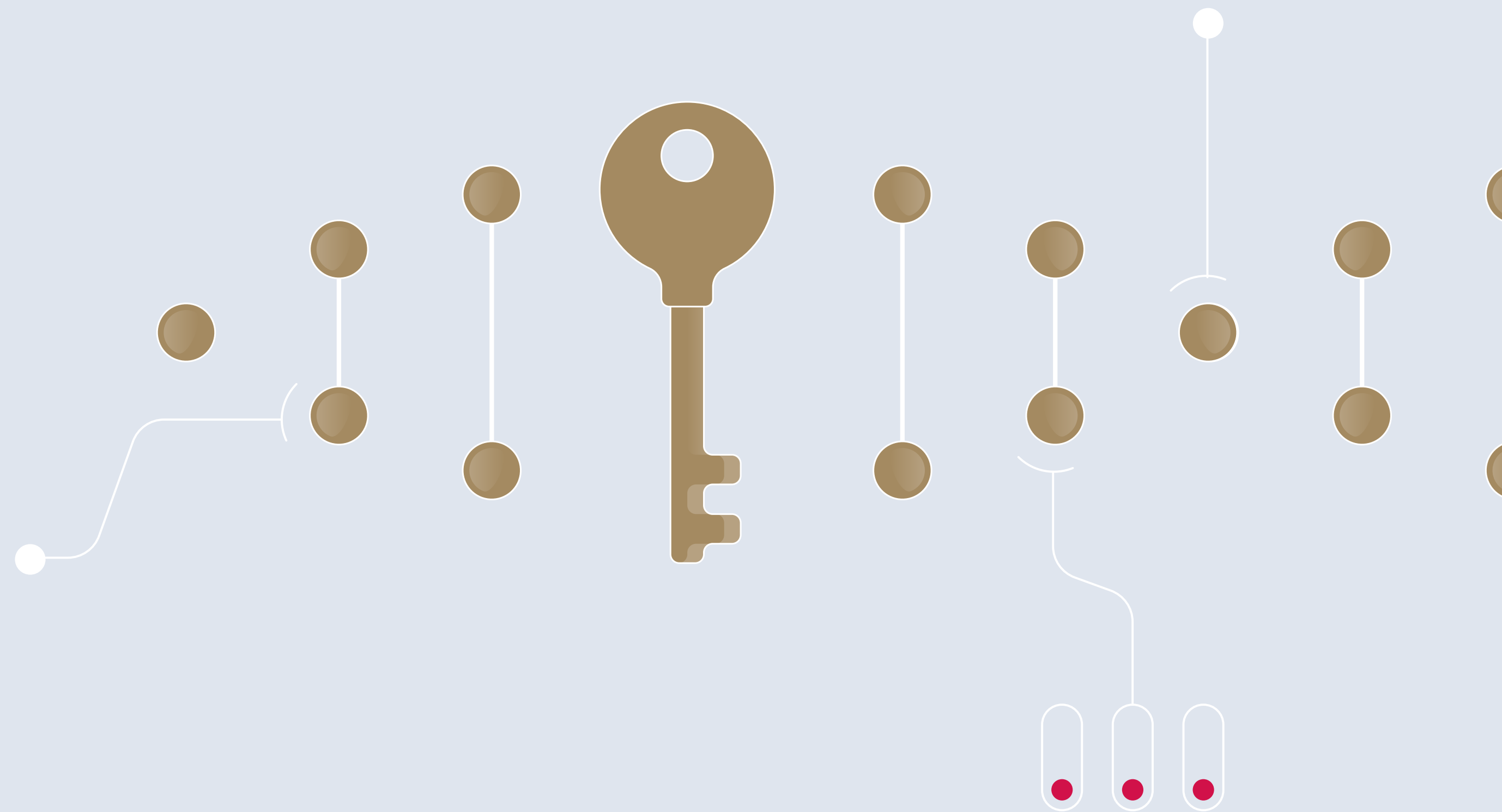
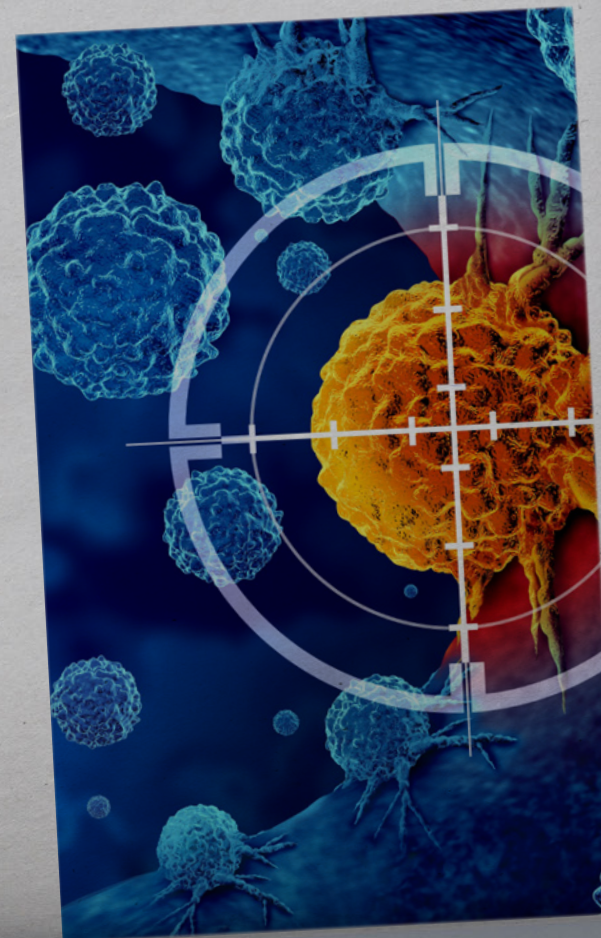


Beskyt dansk bioteknologi og innovation



Dansk startup knækker koden til kræftsygdom



– og udvikler prototypen til et biologisk våben

Når du arbejder med bioteknologi på universiteterne eller i industrien, har du ikke kun ansvar for din faglige integritet, men også for at sikre, at viden og indsigt fra dit arbejde 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 være opmærksom på, bl.a. hvem du samarbejder med, hvilke data og informationer du deler, og hvem der finansierer dine projekter eller din virksomhed. Det gør sig især gældende, hvis du arbejder med bioteknologi med potentiale for dobbelt anvendelse (dual-use). Du bør derfor overveje, om den konkrete viden eller teknologi, du arbejder med, rummer dual-use-potentiale.

Truslen mod bioteknologi i Danmark

Danmark er på nogle områder førende inden for udvikling af bioteknologi, og bioteknologi er et område med stort økonomisk potentiale, men også med dual-use-potentiale, idet en del bioteknologi kan anvendes til militære formål. Derfor er du med dit arbejde en del af et af Danmarks vigtigste, men samtidigt også mest udsatte forsknings- og udviklingsområder.

Din forskning og udvikling kan være et muligt mål for både spionage og uønsket vidensoverførsel fra ikke-ligesindede stater, der ønsker at erhverve sig den nyeste bioteknologiske viden. Hvis dit arbejde ender i de forkerte hænder, risikerer du uforvarende at bidrage til at styrke ikke-ligesindede staters militære kapaciteter eller overvågningsformål.

Dual-use/dobbelt anvendelse:

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



Civilt og militært potentiale

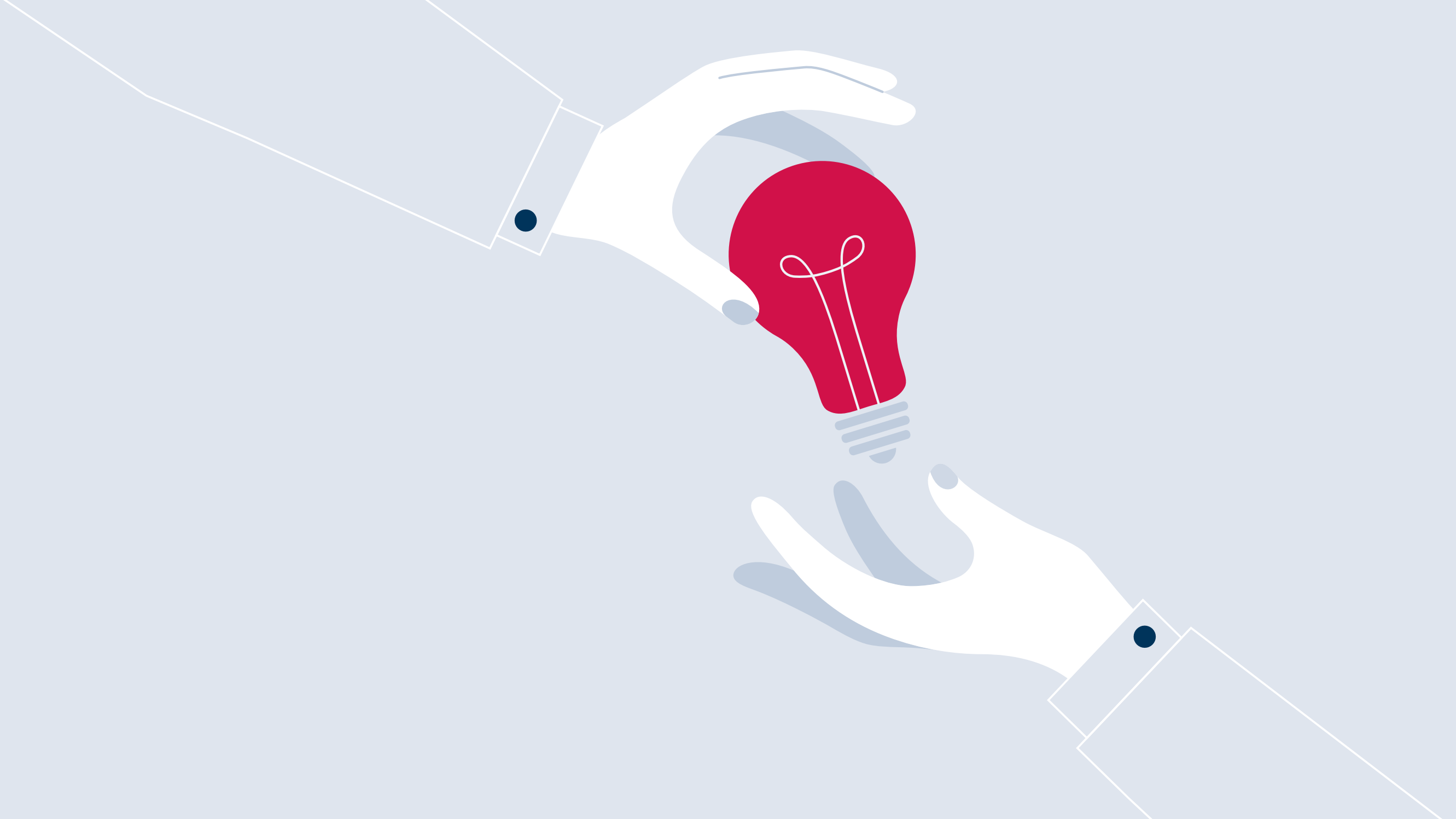
PET vurderer, at bioteknologi som eksempelvis syntetisk biologi og genteknologi har et stort potentiale både civilt og militært. Truslen mod bioteknologi retter sig ikke kun mod den specifikke udvikling af bioteknologi, men også mod beslægtede teknologiområder, der har betydning for udviklingen. Det gælder fx kunstig intelligens, automatisering, robotteknologi og cloud-teknologi.

Fremmede staters interesse

Særligt Kina satser på bioteknologi med militære formål for øje, og det er PET's vurdering, at Kina er villig til at gå meget langt for at erhverve sig viden på de områder, som Kina prioriterer strategisk, hvilket bl.a. gælder bioteknologi. Også Rusland og Iran har udvist interesse for bioteknologi med dual-use-potentiale.

Kontakt og ressourcer:

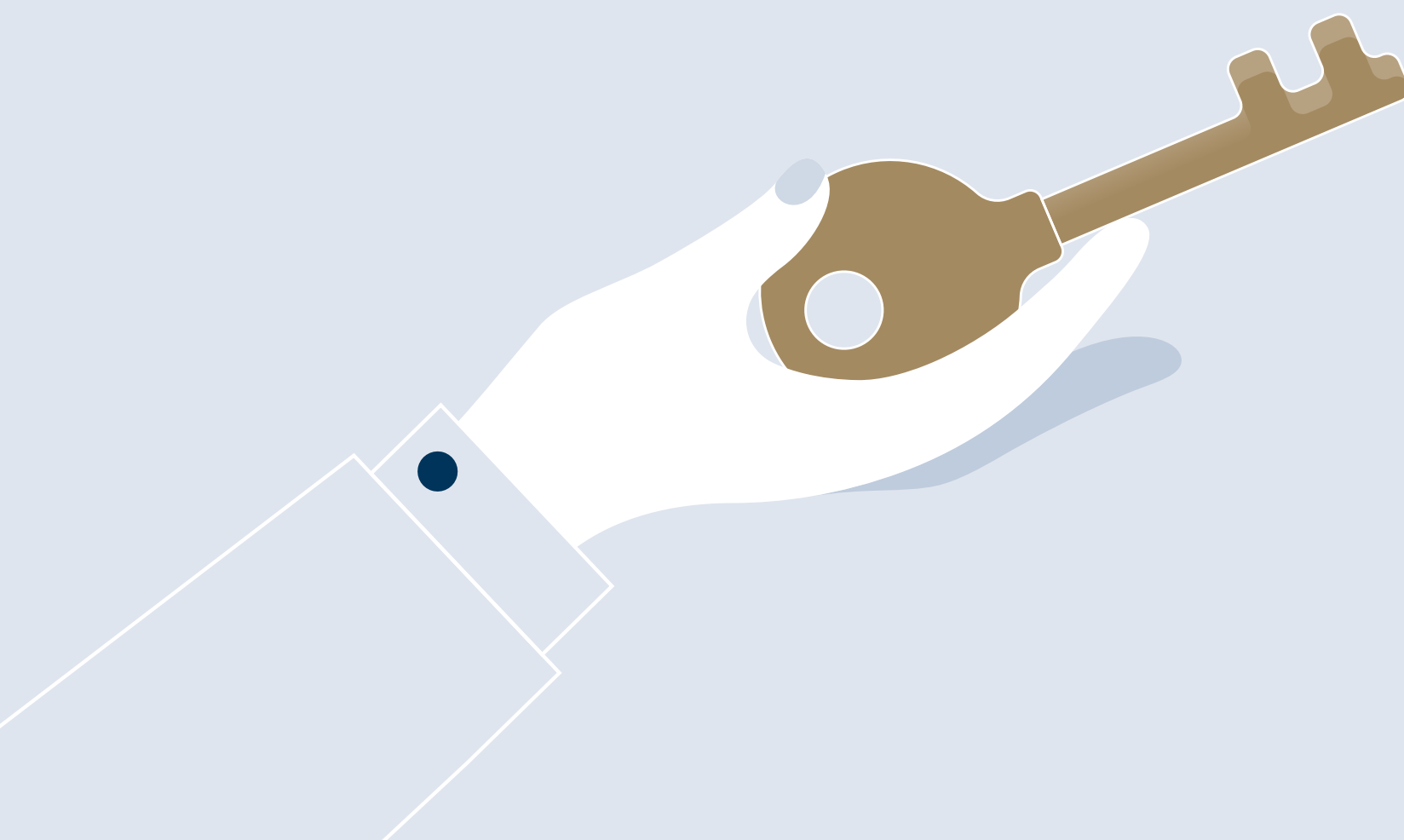
www.pet.dk/sikkerinnovation



Ulovlig vidensoverførsel er i strid med fx spionage- eller eksportregler, mens **uønsket vidensoverførsel** finder sted, når teknologien ikke er reguleret, men kan stride mod Danmarks strategiske interesser. Uønsket vidensoverførsel sker bl.a. i forbindelse med forsknings- eller erhvervssamarbejder inden for det bioteknologiske område.

Hvad kan du gøre?

For at vurdere, om det er risikoen værd at lukke andre ind i dit bioteknologiske miljø, 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-ligesindede stater som Kina og Rusland, der også gerne vil være førende inden for bioteknologi 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

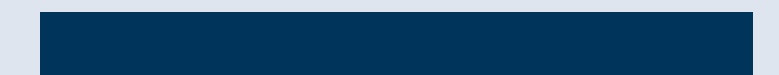
Overvej, hvor meget du ved om nye samarbejdspartnere. Det er vigtigt, at du kender deres baggrund – også de dele, de ikke selv fortæller dig om. Dybere viden om dine eventuelle samarbejdspartneres baggrund ruster dig til bedre at kunne vurdere, om de fx har forbindelse til ikke-ligesindede staters militær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

04 Digitale, faglige og fysiske adgangsveje til dit arbejde igennem samarbejdet

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

