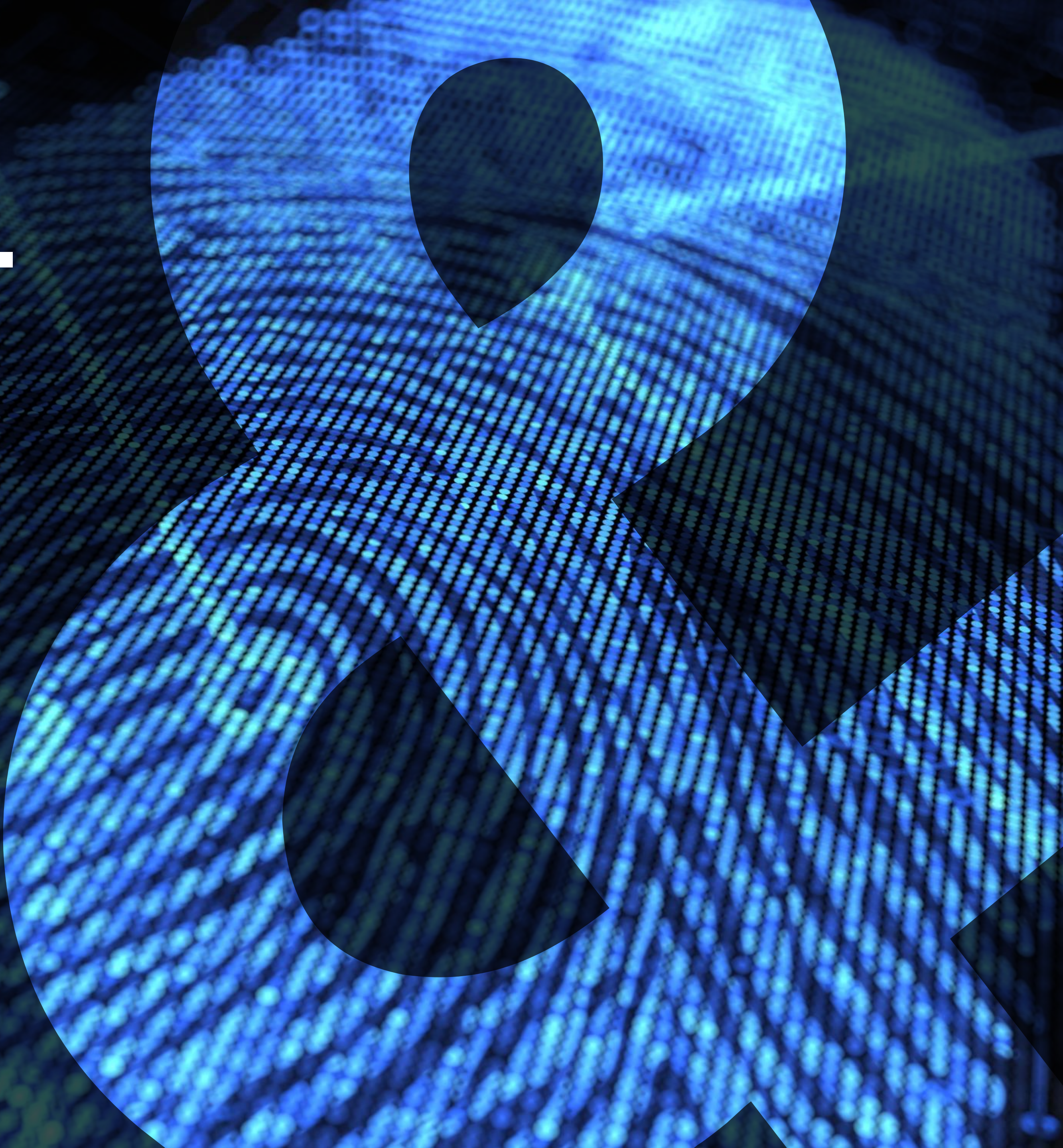
strategy&
Part of the PwC network

eID Country Report 2024

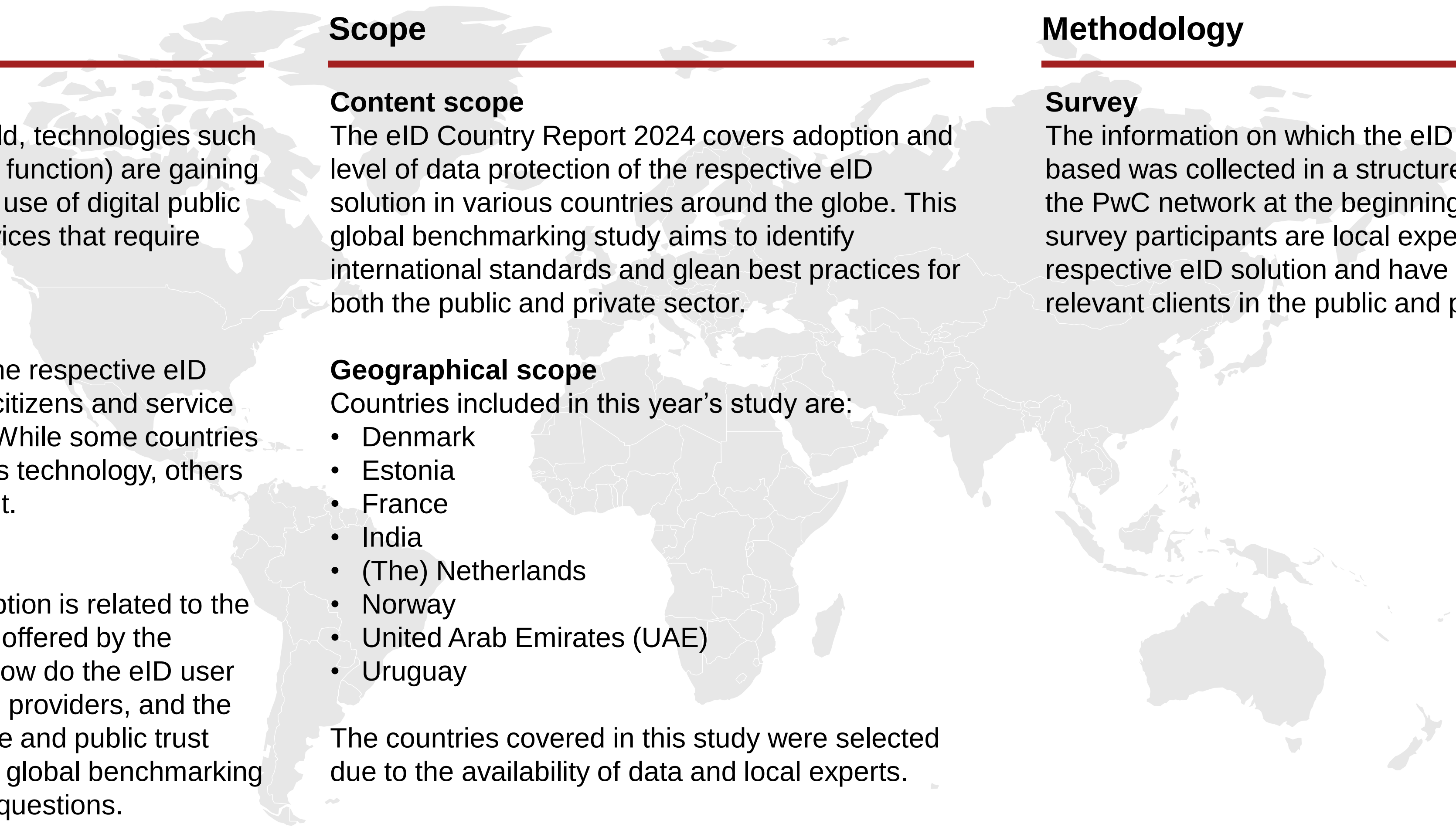
Adoption and data privacy in a digitized world –
a global benchmarking study

April 2024



The eID Country Report 2024 – a survey-based benchmarking study on the global state of adoption and level of data privacy

Introduction and methodology



Relevance

Digitized world
In an increasingly digitized world, technologies such as the eID (online identification function) are gaining in importance. eID enables the use of digital public services as well as private services that require identification.

Status of adoption
However, the extent to which the respective eID solutions are adopted by both citizens and service providers varies considerably. While some countries are regarded as pioneers in this technology, others are still struggling to introduce it.

Level of data privacy
This report examines how adoption is related to the level of data privacy protection offered by the respective local eID solution. How do the eID user rate, the number of eID service providers, and the level of data privacy compliance and public trust correlate with each other? This global benchmarking study examines this and other questions.

Scope

Content scope
The eID Country Report 2024 covers adoption and level of data protection of the respective eID solution in various countries around the globe. This global benchmarking study aims to identify international standards and glean best practices for both the public and private sector.

Geographical scope
Countries included in this year’s study are:

- Denmark
- Estonia
- France
- India
- (The) Netherlands
- Norway
- United Arab Emirates (UAE)
- Uruguay

The countries covered in this study were selected due to the availability of data and local experts.

Methodology

Survey
The information on which the eID Country Report is based was collected in a structured survey within the PwC network at the beginning of 2024. The survey participants are local experts for the respective eID solution and have worked with relevant clients in the public and private sector.

Data privacy compliance builds trust, fostering eID adoption

Executive summary

1 **eID technology is gaining in importance, but the level of adoption varies**
Although eID technology is becoming increasingly important in a digitized world, its level of adoption varies greatly even in developed countries, where user rates sometimes fall below 20% of the respective total population.

2 **Global eID champions focus on data privacy and service offering**
An analysis of countries with the highest user rates (an average of 87%) reveals that they offer both a high level of data privacy compliance (an average of 4.6 on a scale of 5) and a variety of services (+100 service providers on average).

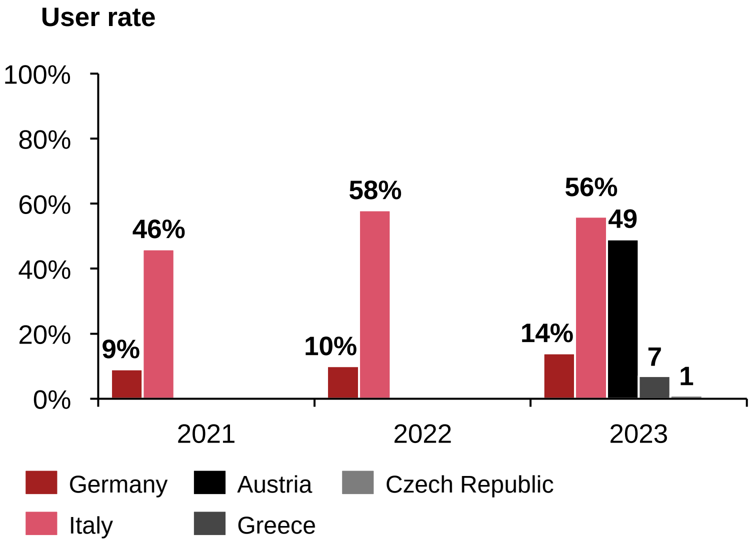
3 **Data privacy compliance is the foundation of trust**
The analysis of eID champions demonstrates that a high level of data privacy compliance has a significant impact on trust (average level of 90%), which in turn is reflected in high user rates. The number of service providers is also correlated with trust levels.

4 **eID laggards should urgently tackle data privacy**
Countries with stagnating user rates should therefore identify data privacy as a critical factor in boosting adoption. They should continually monitor and enhance data privacy to ensure a trust-building ecosystem, facilitating successful public digitization.

Recent data suggests that data privacy compliance could well boost eID user rates in laggard countries

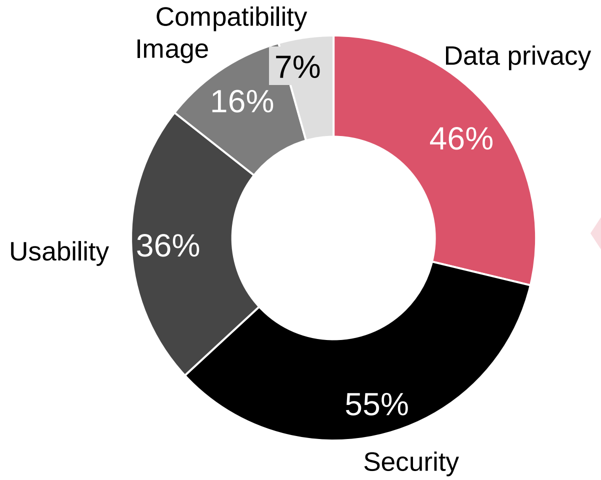
Road to adoption

Stagnating user rates



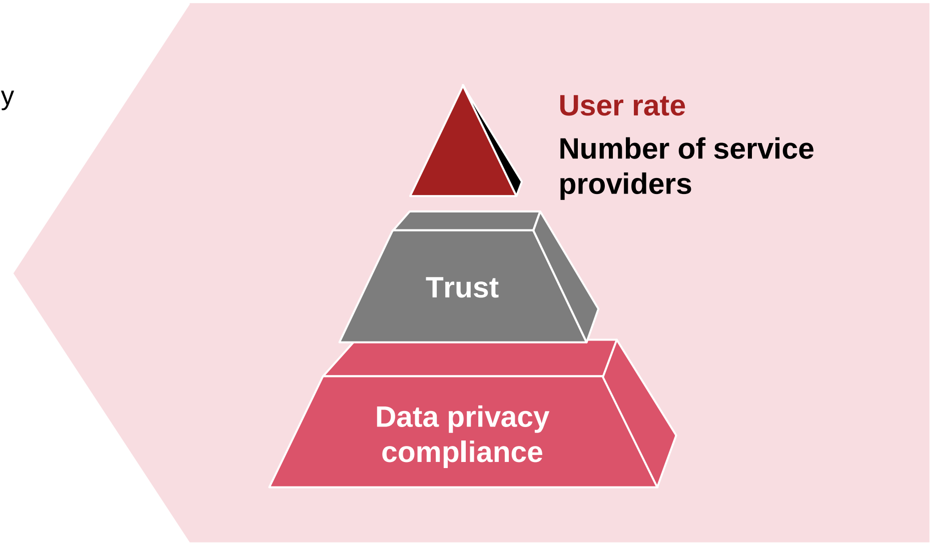
- In an increasingly digitized world, eID is **gaining in importance** because it enables the use of **public and private digital services** that require identification
- However, the extent to which eID is **adopted by citizens varies considerably**, even among developed countries such as Austria, Germany and Italy
- But why are **user rates** and number of service providers for such an important future technology **stagnating**?

Trust drivers



- Recent survey data[1] from Germany on comparable technologies shows that **data protection** is the **most important trust driver, together with** security
- This finding gains further significance when one considers another German study[2] where respondents cited **lack of trust as a top 5 reason** why they do not use eID
- Moreover, the German government's digital strategy[3] also points to **data privacy as the foundation for trust**

Foundation for trust?



- But do global eID leaders really ensure a **high level of data privacy compliance,** and does data privacy compliance really **build trust**?
- Do data privacy compliance and trust affect eID **user rates** and the **number of service providers**?
- And if so, **what actions do eID laggard countries really need to take** in order to increase user rates and the number of service providers?

[1] IDnow Digital Identity Index 2023 Germany; [2] eGovernment MONITOR 2023; [3] Digital Strategy of Germany (2023), p. 11

All our hypotheses on the link between adoption and data privacy compliance are based on key metrics

Establishing the connection

	Key metrics			
Description	**User rate**	**Number of service providers**	**Data privacy compliance**	**Level of trust**
Definition	Metric reveals the **percentage** of respective **total population** using the eID solution	Metric sets out **how many eID services** are available in the respective country	Metric evaluates the **compliance** of the respective eID solution with the **applicable data privacy laws**	Metric refers to **degree of trust** of the respective population in the **data privacy compliance** of the local eID solution
Data	User rate of respective eID was taken from **official sources** and is as up to date as possible	Number of service providers was reached through **official sources** and **expert estimates**	Level of data privacy compliance is based on **expert estimates**	Level of trust in data privacy compliance is also based on **estimates of local experts**
Hypothesis	The user rate depends not only on the **eID services** available, but also on the **level of trust**	**High levels of data privacy compliance** and **trust** also have a positive effect on the number of service providers	Data privacy compliance of the eID solution **increases the level of trust** among citizens	There is a **positive correlation** between the level of trust and the user rate of the eID solution
Chapter	**State of adoption**		**Level of data privacy**	

State of adoption

France

Overview

Official name	France Identité
Year introduced	2019
Responsible institution	Ministry of Interior
Eligibility to use	National citizens, local residents
Documents linked to	National identity card, residence permit
Data privacy framework	GDPR

France Identité allows for a significant number and wide range of services

France Identité

State of adoption

User rate (as % of total population)	~59%
Number of service providers	101+

Top use cases

- Applying for voting proxy
- Accessing the justice portal
- Accessing shared medical records
- Utilizing notary services

Initial challenges

- Lack of social acceptance and adjustment due to fear of public intrusion
- Establishment of national industrial eID ecosystem with common vision and standards
- Maturity of relevant digital use cases justifies the need for secure ID solution

Estonia

Overview

Official name	ID card Mobile ID
Year introduced	2002 (ID card) 2010 (Mobile ID)
Responsible institution	Ministry of Interior
Eligibility to use	National citizens Local residents
Documents linked to	National identity card citizenship card residence permit
Data privacy framework	GDPR

Estonia's ID card and Mobile ID are regarded as Europe's frontrunners

ID card and Mobile ID

State of adoption

User rate (as % of total population)	~84%
Number of service providers	501+

Top use cases

- Filing tax reports
- Using banking services
- Logging in to business register
- Logging in to patient portal
- Receiving medical prescriptions

Initial challenges

- Lack of available digital services, which require an eID to log in
- Keeping up with demand for new electronic services as the user rate increased
- Technological compatibility issues with commonly used plat-forms (browsers, opera-ting systems, etc.)

Denmark

Overview

Official name	MitID
Year introduced	2010
Responsible institution	Danish Agency for Digital Government
Eligibility to use	National citizens, local residents, organizations
Documents linked to	Passport
Data privacy framework	GDPR

By working with financial services providers, MitID unlocked its potential

MitID

State of adoption

User rate (as % of total population)	~88%
Number of service providers	101+

Top use cases

- Making use of public services
- Using Danish banking services
- Using Danish insurance services
- Scheduling with private doctors
- Shopping on private websites

Initial challenges

- By working with the Danish financial sector, attracting active users through eID login to online banking
- Unsuitable technology as the eID was based on Java, which was not available on mobile devices
- Lack of available digital public services that require an eID to log in

Netherlands

Overview

Official name	DigiID eHerkenning
Year introduced	2003 (DigiID) 2011 (eHerkenning)
Responsible institution	Ministry of the Interior and Kingdom relations
Eligibility to use	National citizens (DigiID) organizations
Documents linked to	National identify card, passport, other
Data privacy framework	GDPR

Both DigiID and eHerkenning allow for a significant level of adoption

DigiID and eHerkenning

State of adoption

User rate (as % of total population)	~90%
Number of service providers	101+

Top use cases

- Filing tax reports
- Using local government services
- Accessing social security services
- Accessing student services and loans
- Logging in to healthcare services

Initial challenges

- Overall lack of digital literacy among end users
- Digi-accessibility for potential end users with disabilities
- Bumpy connection process for organizations (eHerkenning)

Norway

Overview

Official name	MinID
Year introduced	2008
Responsible institution	The Norwegian Digitalisation Agency
Eligibility to use	National citizens, local residents
Documents linked to	None
Data privacy framework	GDPR

Because of fierce private competition, public MinID's user rate is below average

MinID

State of adoption

User rate (as % of total population)	~97%
Number of service providers	51-100

Top use cases

- Logging in to online banking
- Making use of public services
- Logging in to healthcare services
- Signing official documents
- Identifying in work context

Initial challenges

- Fierce competition with private eID solutions (e.g., Commfides, Buypass and BankID)
- Cumbersome paper-based registration process using mailed pin-code sheet
- Mistrust as public eID solution MinID provides for only *Substantial* Assurance

India

Overview

Official name	Aadhaar
Year introduced	2009
Responsible institution	Unique Identification Authority of India
Eligibility to use	National citizens, local residents
Documents linked to	None
Data privacy framework	Digital Personal Data Protection (DPDP) Act

Aadhar is among the most adopted eID solutions in the world

Aadhaar

State of adoption

User rate (as % of total population)	~94%
Number of service providers	101+

Top use cases

- Accessing social security services
- Utilizing eSign functionalities
- Making use of public services
- Using banking services
- Accessing telco services

Initial challenges

- Inadequate technical options to enroll in Aadhaar and update data
- Errors with biometric authentication via fingerprints or iris scan
- Linking of eID solution with services for which it is technically not mandatory

Uruguay

In terms of user rate, Uruguay's eID solution is the most advanced in LATAM

IAS CLASSIC v4

Overview

Official name	IAS CLASSIC v4
Year introduced	2015
Responsible institution	AGESIC
Eligibility to use	National citizens, local residents, organizations
Documents linked to	National identity card, citizenship card, residence permit
Data privacy framework	International Civil Aviation Organization (ICAO) Doc 9303

State of adoption

User rate (as % of total population)	~85%
Number of service providers	11-50

Top use cases

- Identifying for digital services
- Reducing the risk of identify theft
- Utilizing eSign functionalities

Initial challenges

- Initial cyber security incidents such as malware, spam and phishing
- Regulatory compliance challenges with regard to modern eGovernment
- Reputational damage due to dubious deals by private service providers

United Arab Emirates

Overview

Official name	Emirates ID
Year introduced	2006
Responsible institution	Federal Authority for Identity and Citizenship
Eligibility to use	National citizens, local residents
Documents linked to	National identity card, passport, citizenship card, residence permit
Data privacy framework	Personal Data Protection Law (Federal Decree Law No. 45 of 2021)

With 100% user rate, Emirates ID is the most popular eID solution in the world

Emirates ID

State of adoption

User rate (as % of total population)	~100%
Number of service providers	501+

Top use cases

- Using local public services
- Using banking services
- Logging in to healthcare services
- Accessing telco services
- Managing employment and businesses

Initial challenges

Ensuring widespread awareness of eID's importance among the whole population

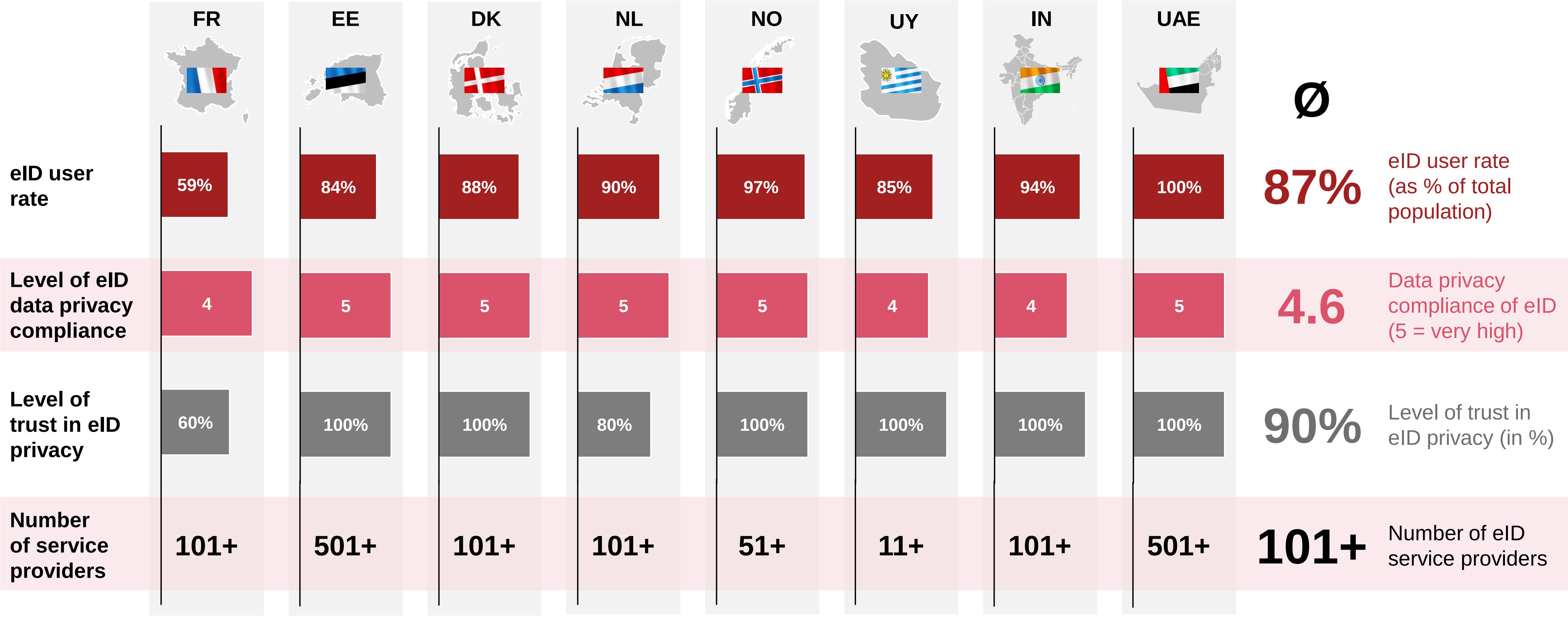
Overcoming significant logistical and operational challenges in order to implement Emirates ID

Establishing a legal and regulatory framework that supports the objectives of Emirates ID while protecting individual rights

Level of data privacy

The results from most of the surveyed countries confirm their reputation as global champions in eID technology

Results overview



	FR	EE	DK	NL	NO	UY	IN	UAE	Ø	
eID user rate	59%	84%	88%	90%	97%	85%	94%	100%	87%	eID user rate (as % of total population)
Level of eID data privacy compliance	4	5	5	5	5	4	4	5	4.6	Data privacy compliance of eID (5 = very high)
Level of trust in eID privacy	60%	100%	100%	80%	100%	100%	100%	100%	90%	Level of trust in eID privacy (in %)
Number of service providers	101+	501+	101+	101+	51+	11+	101+	501+	101+	Number of eID service providers

Source: PwC Strategy& analysis

eID frontrunners take various technical and other measures in order to comply with data privacy requirements

Data privacy compliance

	Technical measures						Other measures	
Country	Encryption	Two-factor authentication	Password policies	Biometric authentication	Tokenisation	Right to view + manage data	Data privacy certification	Body to collect + manage data
DK	✓	✓	✗	✗	✗	✓	✓	Public
EE	✓	✓	✓	✗	✓	✓	✓	Public private partnership
FR	✓	✓	✗	✓	✗	✓	✓	Public private partnership
IN	✓	✓	✓	✓	✓	✓	✗	Public private partnership
NL	✓	✓	✓	✗	✓	✓	✓	Public
NO	✓	✓	✓	✓	✓	✓	✓	Public
UAE	✓	✓	✓	✓	✓	✗	✓	Public
UY	✓	✓	✓	✓	✓	✓	✓	Public

Key observations

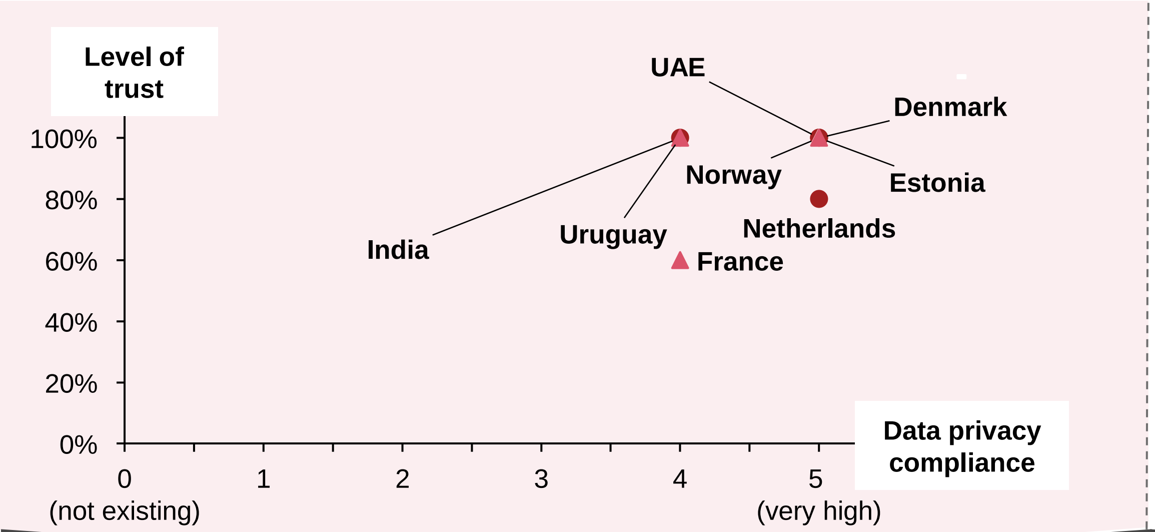
- Global eID frontrunners have **almost all possible technical measures** in place – especially Norway, which has a 97% user rate
- **Privacy-sensitive biometric authentication** is rarely used in European and GDPR-regulated countries
- On the other hand, almost all countries, especially the GDPR-regulated ones, provide for **data privacy certification** (e.g. eiDAS)
- Vast majority of global eID frontrunners are **publicly managed**, although **private service providers** are also used in most of these countries

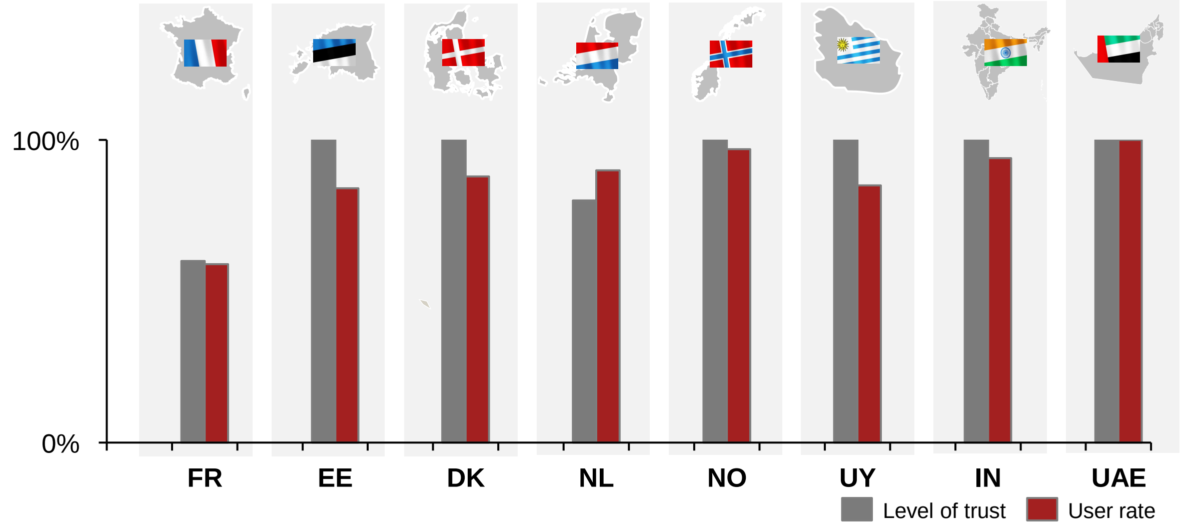
Results show that data privacy compliance correlates positively with trust levels, in turn increasing user rate

Relationship between data privacy compliance, level of trust and user rate

Compliance | Level of trust | User rate

Analyses





Key observations

- Overall, **high levels of data privacy compliance** and **trust in eID privacy** are evident across the surveyed countries: **50%** of these **countries** demonstrate a **strong commitment** to both **data privacy compliance** and **trust**
- Survey results suggest a **potential positive correlation**, implying that higher data privacy compliance may align with elevated trust levels
- Administrators should therefore **take data privacy seriously** as a **trust-building factor,** and design respective eID solutions in a **compliant way**

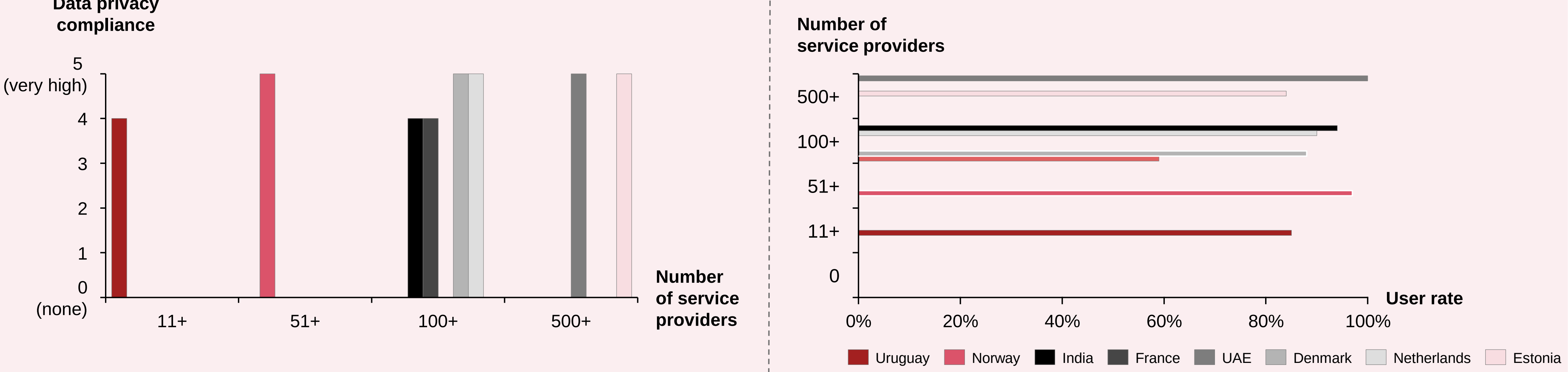
- Survey results suggest a **positive correlation between level of trust and user rates**, with trust levels averaging only 3% higher than user rates
- Therefore, the users' level of trust in the **publicly provided infrastructure** is a **key success factor** for eID solutions
- However, with countries displaying both high levels of trust and high user rates, it is important to explore **additional factors**, such as the **number of service providers**, thus ensuring a thorough analysis

Insights reveal a positive relationship between service provider quantity, compliance and user rate, albeit with some variability

Link between data privacy compliance, number of service providers and user rate

Compliance | Number of service providers | User rate

Analyses



Key observations

- Across all surveyed countries, it can be observed that a **large number of providers (mostly 100+) offer eID services**
- Our results suggest that **countries with a higher level of data privacy compliance** tend to boast a **larger number of service providers**
- Generally, however, there is evidence to suggest that **service providers are also reassured** by a **data privacy-compliant regulatory environment**

- Overall, there is a **positive trend** in the **eID user rate as the number of eID service providers increases**: Countries with **>100** service providers report the **highest user eID rates,** underscoring the **positive impact** of **service diversity on user engagement**
- Therefore, regulators should **create an environment** in which providers are encouraged to offer a wide range of **eID services**

In order to establish a secure and user-friendly eID solution, four best practices are critical to success

Recommendations

1 Data protection by design and default

- In order to establish trustworthy and compliant eID-solutions, **privacy requirements should be considered right at the outset**
- Privacy **principles can be particularly helpful in guiding** how to design and implement eID-solutions and their technical infrastructure

2 Risk assessments and measures

- When processing personal data, **appropriate risk assessments must be carried** out before the processing is initiated
- A **thorough analysis** helps to **ensure that any risks are recognised** at an early stage and that **suitable mitigation measures can be decided on** as early as possible
- **Responsible handling** of privacy risks **strengthens customer confidence** and builds trust for new products

3 Thorough documentation and overview

- Thorough, **precise, and transparent documentation** is a **statutory requirement** and is **crucial for ensuring compliance of nationwide projects**, allowing stakeholders to meet their obligations and be accountable to authorities
- Complete documentation also ensures that a **holistic overview of complex infrastructure, dependencies** and **implementation of privacy requirements is provided**

4 Continual monitoring and enhancement

- Long-term projects and **infrastructure development** offer **constant opportunities** to identify the need for improvement and establish how optimisation can be achieved
- Monitoring and **enhancement processes involving all stakeholders should be agreed** at an early stage

Data protection and privacy should be utilised as key success factors in bolstering user attractiveness

Data protection and privacy as critical success factors

Data protection and privacy have become a **critical element in customer and user trust**

A **lack** of necessary **data protection awareness** can **lead** to the **failure of a product launch** and cause lasting damage to trust and accountability

Growing data protection awareness

Growing awareness leads to more frequent assertion of data subject rights, fostering trust in public bodies and stakeholders when they comply with legal processes to meet user expectations

Safeguarding the reputation of all stakeholders

Maintaining the reputation of all involved stakeholders benefits ongoing and future projects

Responsibility for governments to comply

Government bodies, and their IT solutions, have a general obligation to comply with legal requirements

Alternativ-Vorschlag vorherige Seite

Data protection and privacy should be utilised as key success factors in bolstering user attractiveness

Data protection and privacy as critical success factors

Data protection and privacy have become a **critical element in customer and user trust**

A **lack** of necessary **data protection awareness** can **lead** to the **failure of a product launch** and cause lasting damage to trust and accountability

Growing data protection awareness

Growing awareness leads to more frequent assertion of data subject rights, fostering trust in public bodies and stakeholders when they comply with legal processes to meet user expectations

Safeguarding the reputation of all stakeholders

Maintaining the reputation of all involved stakeholders benefits ongoing and future projects

Responsibility for governments to comply

Government bodies, and their IT solutions, have a general obligation to comply with legal requirements

Our local eID experts are available throughout the world and look forward to talking with you

Lucas Sy
Director, Strategy&

Matthias Bleidiesel
Director, PwC Legal

Niklas Kelbch
Manager, PwC Legal

Lukas David Hoffmann
Senior Associate, Strategy&

Malien Zehnpfenning
Associate, Strategy&

Uruguay

Richard Moreira
Partner
richard.moreira@pwc.com

Jorge Seré
Director
jorge.sere@pwc.com

Rafael Pereira
Manager
rafael.p.pereira@pwc.com

Marcos Gimenez
Director
marcos.gimenez@pwc.com

Netherlands

Pascal Mannot
Partner
pascal.mannot@pwc.com

Jan Visser
Senior Manager
jan.visser@pwc.com

Tosja Selbach
Senior Associate
tosja.selbach@pwc.com

France

Jean-Philippe Duval
Partner
jean.philippe.duval@pwc.com

Norway

Marius Volden
Senior Manager
marius.volden@pwc.com

Trung X. Tran
Director
trung.x.tran@pwc.com

Elisabeth S. Løkkebø
Director
elisabeth.lokkebo@pwc.com

Denmark

Claus Nørklit Roed
Director
claus.norklit.roed@pwc.com

India

Amit Joshi
Director
amit.joshi@pwc.com

Sudhansu Jain
Senior Manager
sudhanshu.jain@pwc.com

Himanshu Wali
Senior Manager
himanshu.wali@pwc.com

Estonia

Kaidi-Kerli Kärner
Partner
kaidi-kerli.karner@pwc.com

United Arab Emirates

Hani Zein
Partner
hani.zein@strategyand.pwc.com

Abdallah Elhor
Director
abdallah.elhor@pwc.com

Alternativ-Vorschlag vorherige Seite

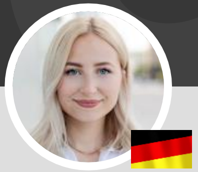
Our local eID experts are available throughout the world and look forward to talking with you

Lucas Sy
Director, Strategy&

Matthias Bleidiesel
Director, PwC Legal

Niklas Kelbch
Manager, PwC Legal

Lukas David Hoffmann
Senior Associate, Strategy&



Malien Zehnpfenning
Associate, Strategy&

Uruguay

Richard Moreira
Partner
richard.moreira@pwc.com

Jorge Seré
Director
jorge.sere@pwc.com

Rafael Pereira
Manager
rafael.p.pereira@pwc.com

Marcos Gimenez
Director
marcos.gimenez@pwc.com

Netherlands

Pascal Mannot
Partner
pascal.mannot@pwc.com

Jan Visser
Senior Manager
jan.visser@pwc.com

Tosja Selbach
Senior Associate
tosja.selbach@pwc.com

France

Jean-Philippe Duval
Partner
jean.philippe.duval@pwc.com

Norway

Marius Volden
Senior Manager
marius.volden@pwc.com

Trung X. Tran
Director
trung.x.tran@pwc.com

Elisabeth S. Løkkebø
Director
elisabeth.lokkebo@pwc.com

Denmark

Claus Nørklit Roed
Director
claus.norklit.roed@pwc.com

India

Amit Joshi
Director
amit.joshi@pwc.com

Sudhansu Jain
Senior Manager
sudhanshu.jain@pwc.com

Himanshu Wali
Senior Manager
himanshu.wali@pwc.com

Estonia

Kaidi-Kerli Kärner
Partner
kaidi-kerli.karner@pwc.com

United Arab Emirates

Hani Zein
Partner
hani.zein@strategyand.pwc.com

Abdallah Elhor
Director
abdallah.elhor@pwc.com

Alternativ-Vorschlag vorherige Seite

Our local eID experts are available throughout the world and look forward to talking with you

Lucas Sy
Director, Strategy&

Matthias Bleidiesel
Director, PwC Legal

Niklas Kelbch
Manager, PwC Legal

Lukas David Hoffmann
Senior Associate, Strategy&

Malien Zehnpfenning
Associate, Strategy&

Uruguay

Richard Moreira
Partner
richard.moreira@pwc.com

Jorge Seré
Director
jorge.sere@pwc.com

Rafael Pereira
Manager
rafael.p.pereira@pwc.com

Marcos Gimenez
Director
marcos.gimenez@pwc.com

Netherlands

Pascal Mannot
Partner
pascal.mannot@pwc.com

Jan Visser
Senior Manager
jan.visser@pwc.com

Tosja Selbach
Senior Associate
tosja.selbach@pwc.com

France

Jean-Philippe Duval
Partner
jean.philippe.duval@pwc.com

Norway

Marius Volden
Senior Manager
marius.volden@pwc.com

Trung X. Tran
Director
trung.x.tran@pwc.com

Elisabeth S. Løkkebø
Director
elisabeth.lokkebo@pwc.com

Denmark

Claus Nørklit Roed
Director
claus.norklit.roed@pwc.com

India

Amit Joshi
Director
amit.joshi@pwc.com

Sudhansu Jain
Senior Manager
sudhanshu.jain@pwc.com

Himanshu Wali
Senior Manager
himanshu.wali@pwc.com

Estonia

Kaidi-Kerli Kärner
Partner
kaidi-kerli.karner@pwc.com

United Arab Emirates

Hani Zein
Partner
hani.zein@strategyand.pwc.com

Abdallah Elhor
Director
abdallah.elhor@pwc.com

strategy&

Part of the PwC network

Thank you

strategyand.pwc.com

Disclaimer: This content is general information purposes only, and should not be used as a substitute for consultation with professional advisors.