

strategy&

Part of the PwC network

eID Country Report

Herausforderungen und Chancen digitaler
Identitäten im internationalen Vergleich

Discover Digital Administration 2025
September 2025

Wir freuen uns, den eID Country Report Ihnen heute vorstellen zu dürfen und auf den gemeinsamen Austausch



Dr. Lukas David Hoffmann
Manager, Berlin

lukas.david.hoffmann@pwc.com
+49 1511 1525178



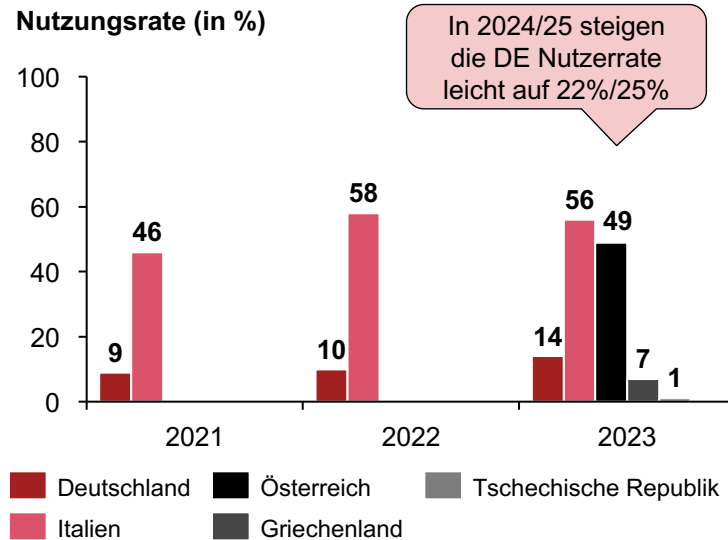
Malien Rosa Zehnpfenning
Senior Associate, Berlin

malien.zehnpfenning@pwc.com
+49 170 7820954

Umfragen legen nahe, dass eine hohe Datenschutzkonformität der eID die Nutzungsrate und Anzahl der Dienstleister steigert

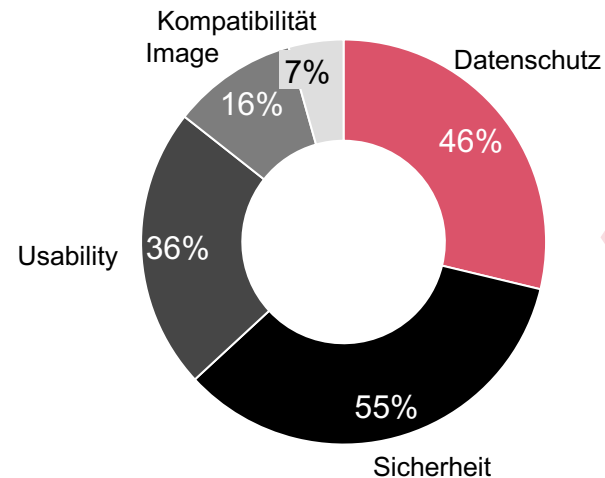
Ausgangspunkt

Stagnierende Nutzerzahlen



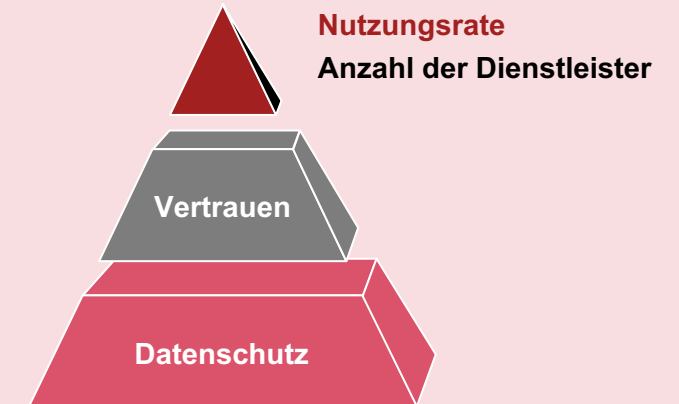
- Zwar **gewinnt** die **eID** auch international zunehmend an **Bedeutung**, doch **wachsen** die **Nutzerzahlen** auch in **entwickelten Ländern** wie Deutschland nur leicht
- **Warum stagnieren die Zahlen der Nutzenden** also trotz Digitalisierung?

Erfolgsfaktoren



- Umfragedaten¹⁾ aus Deutschland zeigen, dass **Datenschutz** neben Sicherheit einer der **wichtigsten Erfolgsfaktoren** ist
- Befragten²⁾ nennen u.a. **die komplexe Anwendung als Grund**, warum sie die eID nicht nutzen – verstärkt durch ein insgesamt geringes Vertrauen in den Staat

Grundlage für Vertrauen?



- Schafft hohe **Datenschutzkonformität** der eID wirklich **Vertrauen**?
- Beeinflusst dies die **Nutzungsrate** und von **Anzahl der Dienstleister**?
- Welche **Maßnahmen** sollten **Nachzügler-Länder** dringend **ergreifen**?

Um diese Hypothese zu testen, haben wir den Country Report erstellt – eine globale, umfragebasierte Studie zur eID

Umfang und Methodik

Relevanz

Bedeutung der eID

In einer zunehmend digitalisierten Welt gewinnen Technologien wie die eID an Bedeutung. Die eID ermöglicht die Nutzung digitaler öffentlicher Dienste sowie privater Dienste, die eine Identifizierung erfordern.

Stand der Adoption

Der Grad der Akzeptanz der jeweiligen eID-Lösungen durch Bürger und Dienstleister ist jedoch sehr unterschiedlich. Während einige Länder als Vorreiter gelten, haben andere noch Schwierigkeiten bei der Adoption.

Relevanz des Datenschutzes

Dieser Bericht untersucht, inwiefern die Akzeptanz mit dem hohen Datenschutzniveau der jeweiligen lokalen eID-Lösung zusammenhängt.

Umfang

Inhaltlicher Umfang

Der eID Country Report zielt darauf ab, internationale Standards zu identifizieren und Best Practices für den öffentlichen und privaten Sektor zu ermitteln.

Geografischer Umfang

- Dänemark
- Estland
- Frankreich
- Indien
- Niederlande
- Norwegen
- Vereinigte Arabische Emirate
- Uruguay

Die in dieser Studie berücksichtigten Länder wurden aufgrund der Verfügbarkeit von Daten und lokalen Experten ausgewählt.

Methodik

Umfrage

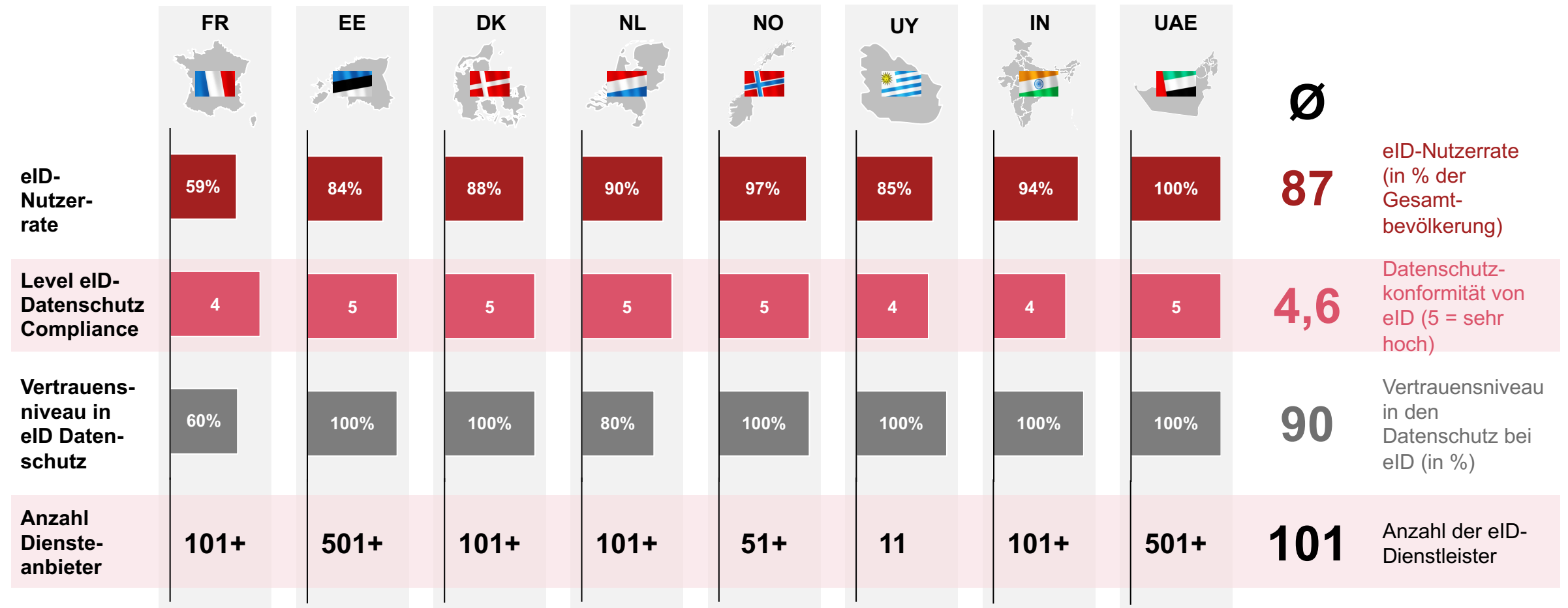
Die Informationen, auf denen dieser Report basiert, wurden 2024 in einer strukturierten Umfrage innerhalb des PwC-Netzwerks erhoben. Die Teilnehmenden der Umfrage sind lokale Experten für die jeweilige eID-Lösung und haben mit relevanten Kunden aus dem öffentlichen und privaten Sektor zusammengearbeitet.

Bewertung

Die Entwicklung der Bewertungsskala erfolgte auf Grundlage umfragebasierter Erfolgsfaktoren aus der einschlägigen Forschung; darauf aufbauend wurde eine eigene Skala (Nutzerrate, Datenschutz-Compliance, Vertrauensniveau, Anzahl Diensteanbieter) konzipiert.









Die Ergebnisse der meisten befragten Länder bestätigen ihren Ruf als globale Spitzenreiter in der eID-Technologie

Übersicht über die Ergebnisse



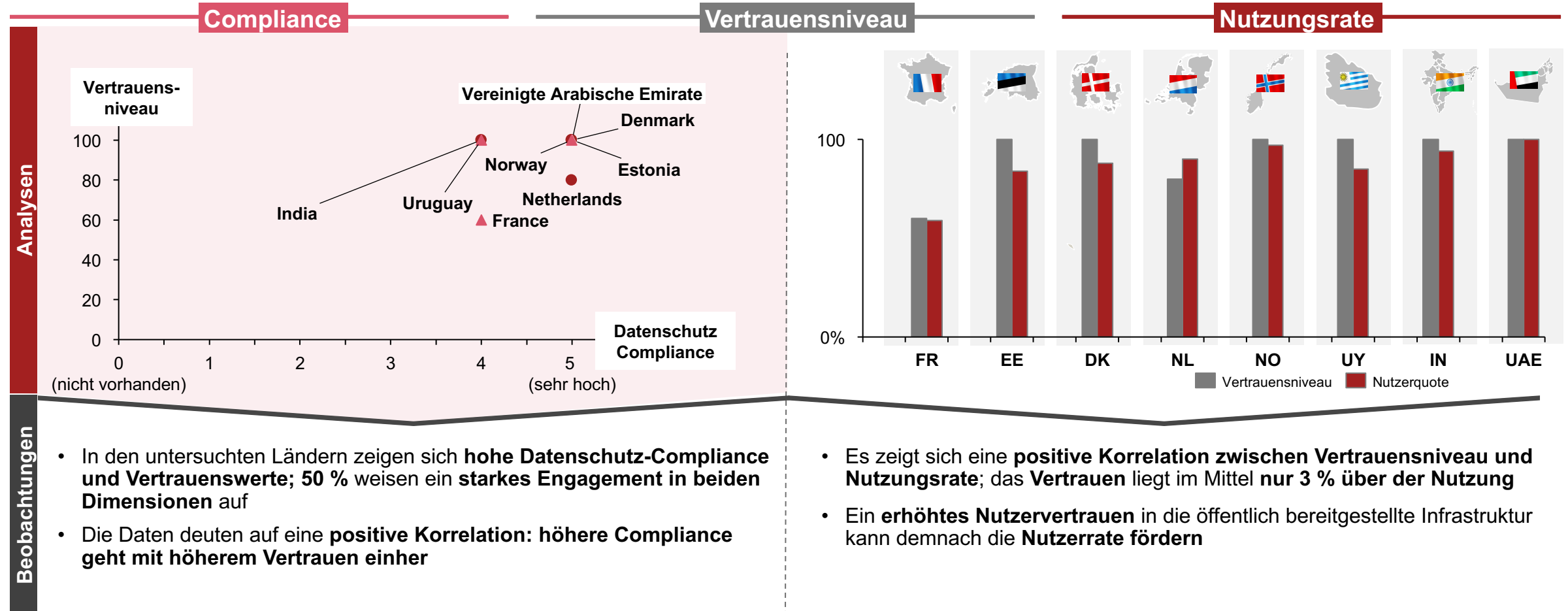
eID-Vorreiter ergreifen verschiedene technische und andere Maßnahmen, um die Datenschutzanforderungen zu erfüllen

Einhaltung der Datenschutzbestimmungen

Land	Technische Maßnahmen						Weitere Maßnahmen		Wichtige Beobachtungen
	Verschlüsselung	Zwei-Faktor-Authentifizierung	Passwortrichtlinien	Biometrische Authentifizierung	Tokenisierung	Recht auf Einsicht der Daten	Datenschutz-zertifizierung	Stelle zur Erhebung/Verwaltung von Daten	
DK 	✓	✓	✗	✗	✗	✓	✓	Öffentlich	<ul style="list-style-type: none"> Führende eID-Anbieter haben nahezu alle verfügbaren technischen Maßnahmen umgesetzt Biometrische Authentifizierung wird in Europa bzw. DSGVO-Ländern seltener eingesetzt Nahezu alle Länder verlangen Konformitäts-/Zertifizierungsnachweise (z. B. im Rahmen eIDAS) Die Mehrheit der führenden eID-Systeme wird öffentlich betrieben; private Dienstleister sind häufig ergänzend eingebunden
EE 	✓	✓	✓	✗	✓	✓	✓	Öffentlich-private Partnerschaft	
FR 	✓	✓	✗	✓	✗	✓	✓	Öffentlich-private Partnerschaft	
IN 	✓	✓	✓	✓	✓	✓	✗	Öffentlich-private Partnerschaft	
NL 	✓	✓	✓	✗	✓	✓	✓	Öffentlich	
NO 	✓	✓	✓	✓	✓	✓	✓	Öffentlich	
VAE 	✓	✓	✓	✓	✓	✗	✓	Öffentlich	
UY 	✓	✓	✓	✓	✓	✓	✓	Öffentlich	

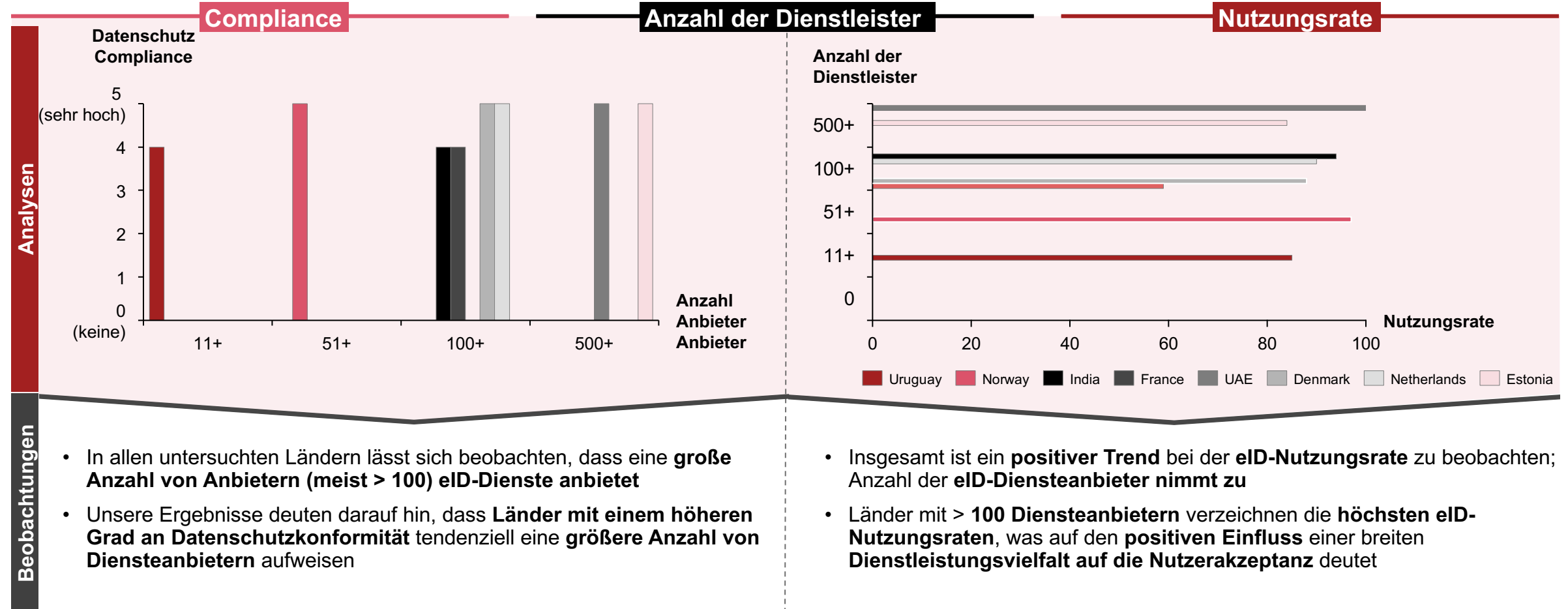
Die Ergebnisse zeigen auch, dass strikte Datenschutz-Compliance das Vertrauen stärkt und damit die eID-Nutzung steigert

Zusammenhang Compliance, Vertrauensniveau, Nutzerrate



Mehr Anbieter und konsequente Compliance korrelieren mit höheren Nutzungsraten – trotz leichter Varianz

Zusammenhang Compliance, Anzahl Diensteanbieter, Nutzungsrate



Die Ergebnisse belegen: eine hohe Datenschutzkonformität ist ein zentraler Treiber der eID-Adoption

Fazit



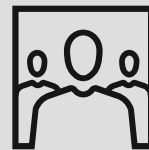
Datenschutzkonformität ist ein entscheidender **Faktor** für das **Vertrauen** von **Nutzenden**.

Ein **mangelndes Bewusstsein** für den notwendigen Datenschutz kann zum **Scheitern einer Technologie** führen und das **Vertrauen nachhaltig schädigen**.



Wachsendes Bewusstsein für Datenschutz

Mit wachsendem Bewusstsein für den Datenschutz werden auch **Betroffenenrechte häufiger durchgesetzt**



Schutz der Reputation aller Beteiligten

Die **Reputationswahrung** aller beteiligten Interessengruppen **kommt laufenden und zukünftigen Technologieprojekten zugute**



Verantwortung der Verwaltung für Compliance

Behörden sind nach dem Grundsatz der Gesetzmäßigkeit der Verwaltung **verpflichtet, gesetzliche Anforderungen einzuhalten**

Um sichere und nutzerfreundliche eID-Lösung zu etablieren, sollten vier Maßnahmen ergriffen werden

Empfehlungen

1

Data Privacy by Design & Default

- **Datenschutzanforderungen** sollten idealerweise bereits **von Anfang an mitgedacht** werden
- Datenschutz kann dabei hilfreich sein, die die **Gestaltung und Umsetzung von eID-Lösungen** und ihrer technischen Infrastruktur zu steuern

2

Risikobewertungen und Maßnahmen

- **Vor** Verarbeitung personenbezogener Daten müssen **Risikobewertungen durchgeführt** werden
- Analyse trägt dazu bei, dass **Risiken frühzeitig erkannt** und **geeignete Maßnahmen** so früh wie möglich **ergriffen** werden können

3

Übersicht und Dokumentation

- **Dokumentation** ist **gesetzlich vorgeschrieben** und von Bedeutung, damit die Beteiligten **gegenüber Aufsichtsbehörden Rechenschaft** ablegen können
- Dokumentation gewährleistet zudem einen **ganzheitlichen Überblick** über **komplexe Infrastrukturen** und **bestehende Abhängigkeiten**

4

Überwachung und Verbesserung

- **Langfristige Projekte** bieten ständig Gelegenheit, **Verbesserungsbedarf zu erkennen** und **festzulegen**, wie Optimierungen erzielt werden können
- **Regelmäßige Überwachungs- und Verbesserungsprozesse**, an denen alle Beteiligten beteiligt sind, sollten **frühzeitig vereinbart** werden



Wer von Ihnen verfügt über eine eID, wer nicht – und aus welchen Gründen?

Vielen Dank

strategyand.pwc.com

© 2025 PwC. Alle Rechte vorbehalten.

PwC bezieht sich auf das PwC-Netzwerk und/oder eine oder mehrere seiner Mitgliedsfirmen, die jeweils eigenständige juristische Personen sind. Weitere Informationen finden Sie unter pwc.com/structure.

Haftungsausschluss: Dieser Inhalt dient ausschließlich allgemeinen Informationszwecken und ersetzt nicht die Beratung durch professionelle Berater.