Potenziale der Datenökonomie besser nutzen

	Situation **Die innovativen Potenziale durch eine sichere, praktikable Nutzung von Daten werden nicht ausgeschöpft.**	Zielsetzung **Sichere digitale Ökosysteme, in denen Daten einfach wertschöpfend genutzt werden können.**	Lösung **Praxisorientierte Unterstützung einer sicheren Nutzung von Daten mit angemessenen Rahmenbedingungen**
Impuls 1 **Datenschutz rechtssicher, praktikabel und wettbewerbskonform gestalten**	1) Unternehmen fehlen praktikable Datenschutzregeln für alltägliche Geschäftsvorfälle (z. B. Websites). Sie klagen über zu umfangreiche Datenschutzpflichten [1](u. a. Information, Dokumentation).	1) Stabile und praktikable Gesetze für elektronische Kommunikation schaffen und unnötige Belastungen reduzieren. Digitale Wettbewerbsfähigkeit schafft Wachstum.	1) ePrivacy zeitnah neu gesetzlich regeln - möglichst EU-weit, mindestens bundesweit. Übermäßige bürokratische Pflichten abbauen.
	2) Deutsche Unternehmen sind auf Drittstaatentransfers angewiesen. Die Konsequenzen des EuGH-Urteils zu Schrems II könnten sich massiv negativ auf die deutsche Wirtschaft auswirken.[2]	2) Rechtsunsicherheit für Drittstaatentransfers sind zeitnah zu beseitigen. Die Maßstäbe der DSGVO sind auf Anpassungsbedarf zu prüfen.	2) Stabilen und praktikablen Rechtsrahmen schaffen - zeitnah über neue Angemessenheitsbeschlüsse (USA), modernisierte Standardvertragsklauseln, langfristig über weltweite Datenschutzstandards.
	3) Die Entwicklung neuer Technologien wie KI und Blockchain stellen Unternehmen vor gewichtige Rechtsfragen (bpsw. Zulässige Nutzung von Daten, Umsetzung von DSGVO-Pflichten).	3) Planungssicherheit schaffen: Datenschutz sollte sich als Wettbewerbsvorteil und nicht als Wachstums- und Innovationsbremse erweisen.	3) DSGVO und Anpassungsgesetzgebung (ePrivacy) von Überregulierung befreien und praxiskonform gestalten, bestehende Geschäftsmodelle erhalten.
Impuls 2 **Sicheres digitales Ökosystem schaffen**	1) Die Vielzahl von Förder- und Info-Angeboten zur IT-Sicherheit von Bund, Ländern sowie privaten Initiativen macht es Unternehmen schwer, passende und gute Hilfestellungen zu finden.	1) Unternehmen sind auf Angriffe und Notfälle vorbereitet und haben eine zentrale Anlaufstelle, über die sie die passenden Informationen und Ansprechpartner finden.	1) Ein zentraler Lotse (Transferstelle IT-Sicherheit) informiert und verweist auf Angebote zur Prävention sowie Hilfe bei Sicherheitsvorfällen.
	2) Auflagen für Unternehmen zu IT-Sicherheit (z.B. Meldepflichten) nehmen zu, ohne dass sie erkennbare Sicherheitsgewinne für die Betriebe bringen.	2) Die Pflichten sind möglichst gering gehalten und zielführend auch zum Nutzen der Unternehmen gestaltet.	2) Gesetze (z. B. IT-SichG 2.0) auf Praxistauglichkeit prüfen und mehr auf Freiwilligkeit und Nutzen für Unternehmen ausrichten (z.B. freiwillige Meldungen statt Meldepflichten bei Vorfällen).
	3) Die EU ist abhängig von Basistechnologien und Standards, die in den USA und Asien entwickelt werden.	3) In der EU werden weltweit konkurrenzfähige, sichere Soft- und Hardwareprodukte hergestellt.	3) Schlüsseltechnologien (z. B. durch die Agentur für Sprunginnovationen) fördern, die der Staat als Pilotnutzer verwendet (IoT, KI, Blockchain). Europäische Anbieter durch gemeinsame Plattform unterstützen.
	4) Unternehmen ist oft unklar, wie sicher die eingekauften und eingesetzten Produkte sind.	4) Es ist für Unternehmen erkennbar und nachvollziehbar, welches IT-Sicherheitsniveau ein IKT-Produkt hat.	4) Gütesiegel einführen, mit denen das IT-Sicherheitsniveau einschätzbar ist.
Impuls 3 **Rohstoff Daten heben**	1) Daten fallen bei den verschiedensten Akteuren an. Sie sind Grundvoraussetzung für digitale Innovationen, werden jedoch oftmals nicht im notwendigen Umfang aufbereitet.	1) Deutschland und die EU sind Vorreiter der Datenwirtschaft. Es stehen ausreichend Daten zum Trainieren von KI und für innovative Produkte zur Verfügung.	1) Wettbewerbsfähige, sichere Infrastruktur und Standards für Datenpools, z.B. mit Gaia X, ausbauen. Rechtliche und steuerliche Anreize für gemeinsame Datennutzung setzen.
	2) Eigene Daten sind aber auch ein Kernelement für die Geschäftsmodelle vieler Unternehmen. Ihre Speicherung und Aufbereitung ist investitionsintensiv.	2) Recht an Daten ist geklärt; Datenkooperationen und Datenpools sind möglich.	2) Faire und klare Regeln für Datenaustausch und -zugang schaffen (z.B. Austausch privilegieren). Dabei Datensouveränität respektieren.
	3) Daten lassen sich ohne Datenverlust teilen. In digitalen Prozessen ist häufig unklar, wer Zugriff auf dabei generierte Daten haben darf.	3) Recht auf Datenzugang und -teilhabe ist abgestimmt.	3) Rechtssicheres Arbeiten mit Big Data, z.B. durch Novelle EPVO & DSGVO. Anreize schaffen für Datenteilhabe & -schnittstellen (z.B. Standards, Datenpools)
	4) In der öffentlichen Verwaltung fallen viele Daten an, die zu wenig und schlecht auffindbar bereit gestellt werden.	4) Leichter Zugang zu “Open Government Data”	4) “Open Government Data” bundes- und EU-weit koordiniert ausbauen.

Ansprechpartner: Sven Kranixfeld, sven.kranixfeld@passau.ihk.de, 0851 507-341

[1] DIHK-Umfrage 2019
[2] Verbändepapier – Forderungen zu Drittstaatentransfers 2020
[3] IHK-Positionspapier „IT-Sicherheit für Unternehmen“