digital chameleon

digital chameleon

Regulatorische Herausforderungen für Cloud Solutions

24. Juni 2021

OUR MISSION

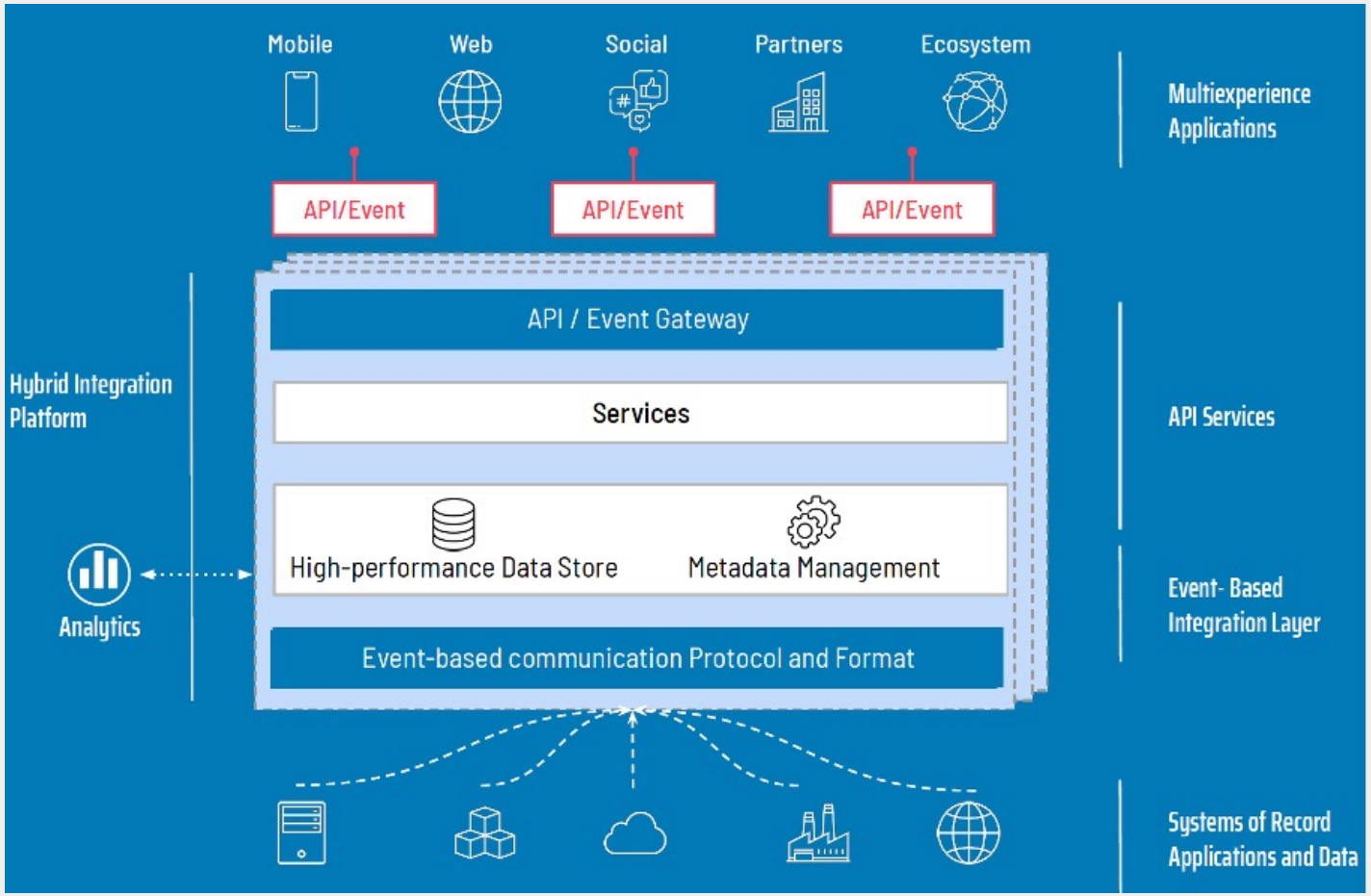
[At Digital Chameleon we are helping to create a better world of effective healthcare by driving change for a connected Digital Health Ecosystem]

digital chameleon

IoT Cloud Plattformen als Treiber der Digitalen Welt

digital chameleon

- Antrieb der Digitalisierung durch **„Smart Connections“ Geschäftsmodelle**
- Verbindung von Geräten mit **cloud-basierten digitalen Plattformen (IoT)**
- Data Collection & Sharing (**Big Data**) angereichert mit **Künstlicher Intelligenz**
- **Smart Home, Industrie 4.0, Smart Banking/ Finance, Smart HR**



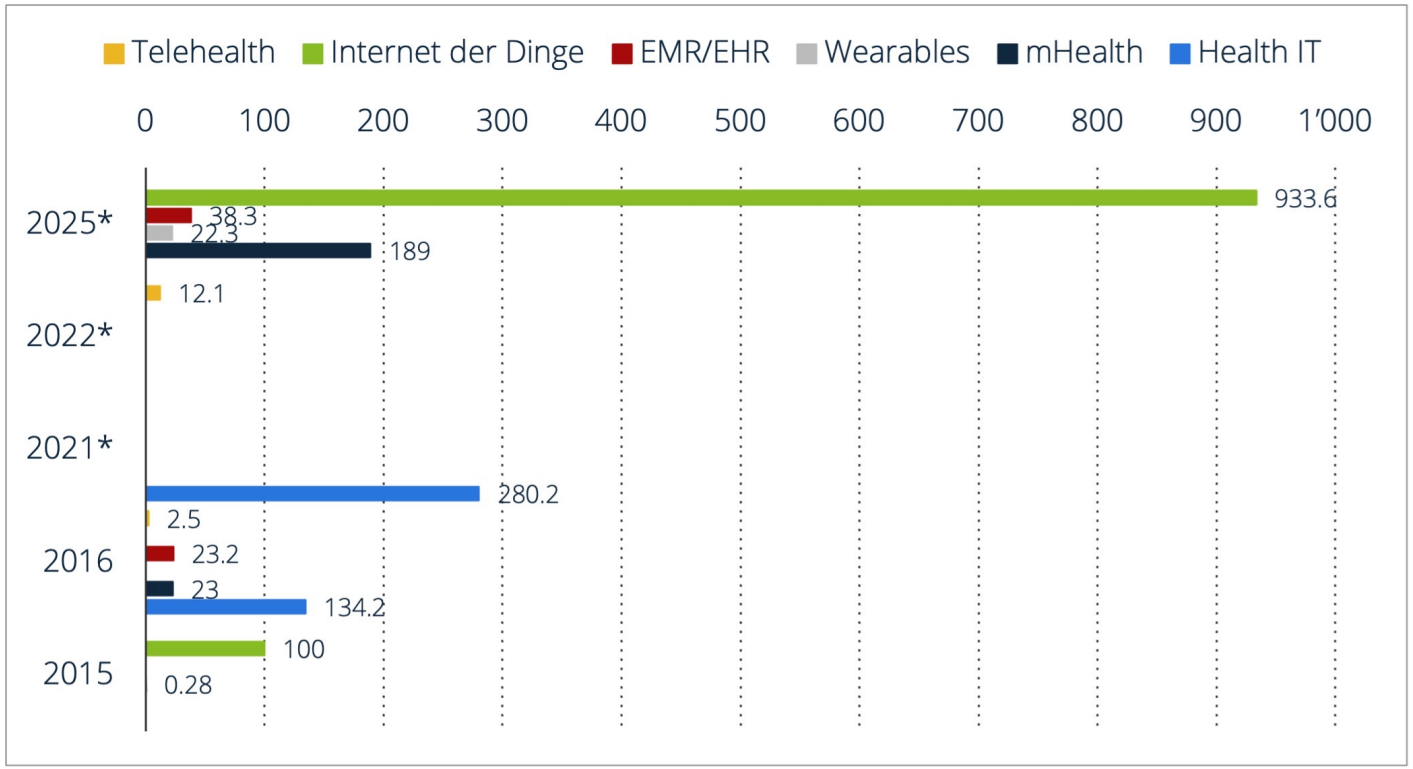
Quelle: Gartner’s Target Architecture: The Digital Integration Hub (DIH)

Digitalisierung am Beispiel Gesundheitswesen

digital chameleon

- Beispiel Gesundheitswesen, weiter angetrieben durch Corona
- Vision eines **„Digital Health Ecosystem“** zur Förderung von medizinischer Forschung & Entwicklung, “Precision & Personalized Medizin“ und Kosteneinsparung im Gesundheitssystem
- Use Case „Real World Data (RWD)“
  - Beispiel Health Data Schweiz: Swiss Personalized Health Network (SPHN):
    “Infrastructure building to enable nationwide use and exchange of health data for research“
  - Beispiel BioMedical Research: Austausch von DNA & Genom Data
- Health Platform / Cloud Service Anbieter: Philipps Healthcare, Siemens Healthineers, BrightInsight

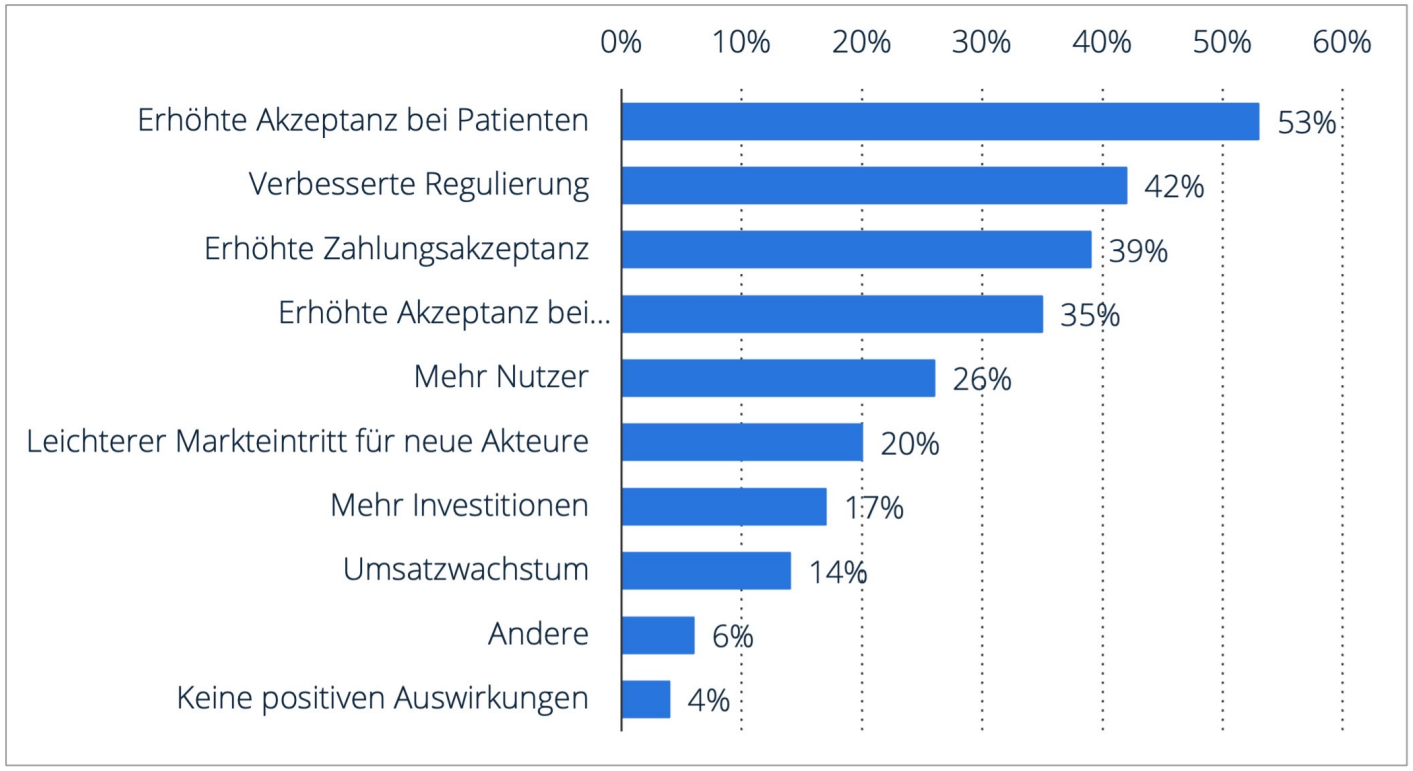
Entwicklung IoMT (cloud-based business models)



Quelle: Capgemini, 22. Oktober 2018, Umsatz des Digital Health-Marktesweltweit nach Segment im Zeitraum der Jahre 2015 bis 2025 (in Milliarden US-Dollar)

- Seit 2015 werden Internet-of-Things (IoT)-Anwendungen zunehmend im Gesundheitswesen entwickelt
- der globale Markt für sogenannte IoMTs soll weiter von 100 Milliarden US-Dollar auf **933,6 Milliarden US-Dollar im Jahr 2025 wachsen**

Akzeptanz von IoMT bei Patienten und Erwartung an verbesserte Regulierung



Quelle: Statista, 2021

- Umfrage zu den positiven Auswirkungen der Corona-Krise auf die Digital Health-Industrie im Jahr 2020

Bedeutung Datensouveränität

digital chameleon

- **Hinterfragung des eigentlichen Business Models**
  - Ist der Zweck wirklich nur der eigentliche Business Case oder doch „Datenklau“? Siehe Cloud Service Provider: Amazon Web Services, Microsoft Azure, Google Cloud Platform
  - Beispiel Business Model „Scooter“ – Tracking von GPS Daten um Konsumverhalten zu evaluieren
- **Benutzer/User von Anwendungen können nicht sicher sein**
  - Wofür die Daten insgesamt genutzt werden (ausserhalb des initialen Use Cases)
  - Welche Daten (genau) genutzt werden (Personendaten, Bilder, Gesprächsverläufe, Standort etc.)
  - Wo (genau) Daten gespeichert werden und wie lange
  - Wer (genau) Zugriff auf Daten und Rechte an Daten hat

Entwicklung weg von Datensouveränität?

- Internationale Beispiele, bei denen Datennutzung ohne vorheriges Einverständnis der Nutzer betrieben wird, **ist dies unsere Zukunft?**
  - Digital Health Forderung: Datennutzung ohne vorheriges Einverständnis zum Wohle der Menschheit (Forschung, Prävention, Heilung)
  - Italien, Österreich, Frankreich etc.: Organspende: automatisch Organspende verpflichtend, kein Opt-in, Opt-out möglich über Widerspruchregister
  - USA, Polen: Strafregister Sexualstraftäter (kein Opt-in, Datenschutz-Rechte wurden Tätern aberkannt)
  - Schweden: Steuerkalender über monatliche Einkünfte & Schulden (Verpflichtend für jeden Ansässigen in Schweden, kein Opt-in/out, Veröffentlichung von Name, Geburtsdatum, Ehestand)

Risiken & Anforderungen/

Cloud Platformen im regulierten Umfeld

Gegenüberstellung: WHO Digital Health Handbook, EU Digital Health & EU Regulation KI & IoT & Robotics

- Wirksamkeit der Lösungen & Geschäftsmodelle
- Patientensicherheit bei Anwendung der Lösung
- Data Integrity & Protection
- IT & Cybersecurity

Organizations	WHO	EU	AIOTA	Patient Safety	Effectivness	Regulatoty Compliance
Risk Categories/ Requirement Areas	Digital Handbook Digital Health Platform: Building a Digital Information Infrastructure (Infostructure) for Health	EU Commission Report on safety and liability implications of AI, the Internet of Things and Robotics	Position Paper on IoT for Europe Digital Health Initiative			
Effectiveness	• Health promotion and disease prevention • Prevention, targeted treatment	• Product Safety •	• Reliability • Accountable •			
Patient Safety	• Patient safety	• Product Safety	• Safety • Accountable •			
Interoperability	• Interoperability	• Openness due to its digital dimension encompassing tangible and intangible elements (software and data). •	• Ability to connect			
Security (IT & Cyber)	• Data security (confidentiality, integrity, and availability)	• Data driven: It entails data generation, data gathering, data processing and data analysis • Cybersecurity risk	• Security			
Data Protection	• Data privacy	• Data driven: It entails data generation, data gathering, data processing and data analysis • Risks of privacy breaches	• Privacy			
Data Integrity	• data quality and reliability • Trustworthy data	• N/A	• N/A			
IT Architecture	• Lack of Infrastructure	• Complexity: Given the numerous interdependencies in the value chain and the variety of actors • Autonomous behaviour: Many of the operations provided through and by an IoT system can be fully autonomous; • Lack of Infrastructure	• N/A			
Costs	• Cost-effectiveness • Affordability	• N/A	• N/A			
Ethics	• Ethics	• N/A	• N/A			

Quelle: Digital Chameleon, 2021

Regulatorische Herausforderungen

- Datenstandards / Daten Evidenz: wie definiert sich dieser Standard und welcher Standard ist akzeptabel, um bestimmte Auswertungen vorzunehmen, insbesondere aus diversen Quellen und Ländern (siehe auch medizinische Forschung & Wissenschaft)?
- Datenintegrität (Pharma): Integrität über den gesamten Data Lifecycle, Single Source of Truth – Original oder Copy? Korrektheit und Vollständigkeit der Daten, zudem Nachweis wer hat Daten erstellt und verändert (Audit Trail)
- Verifizierung & Validierung von Cloud Solutions & Ecosystems: Einheitliche Anforderungen fehlen, durch Komplexität der Systeme & Use Cases, keine einheitlichen Regularien & Standards (sogar in Life Science)
- „Regulatory Convergence“: Regulatorischer „Flickenteppich“, Harmonisierung von Regularien & Standards nötig (Fachlich & International)

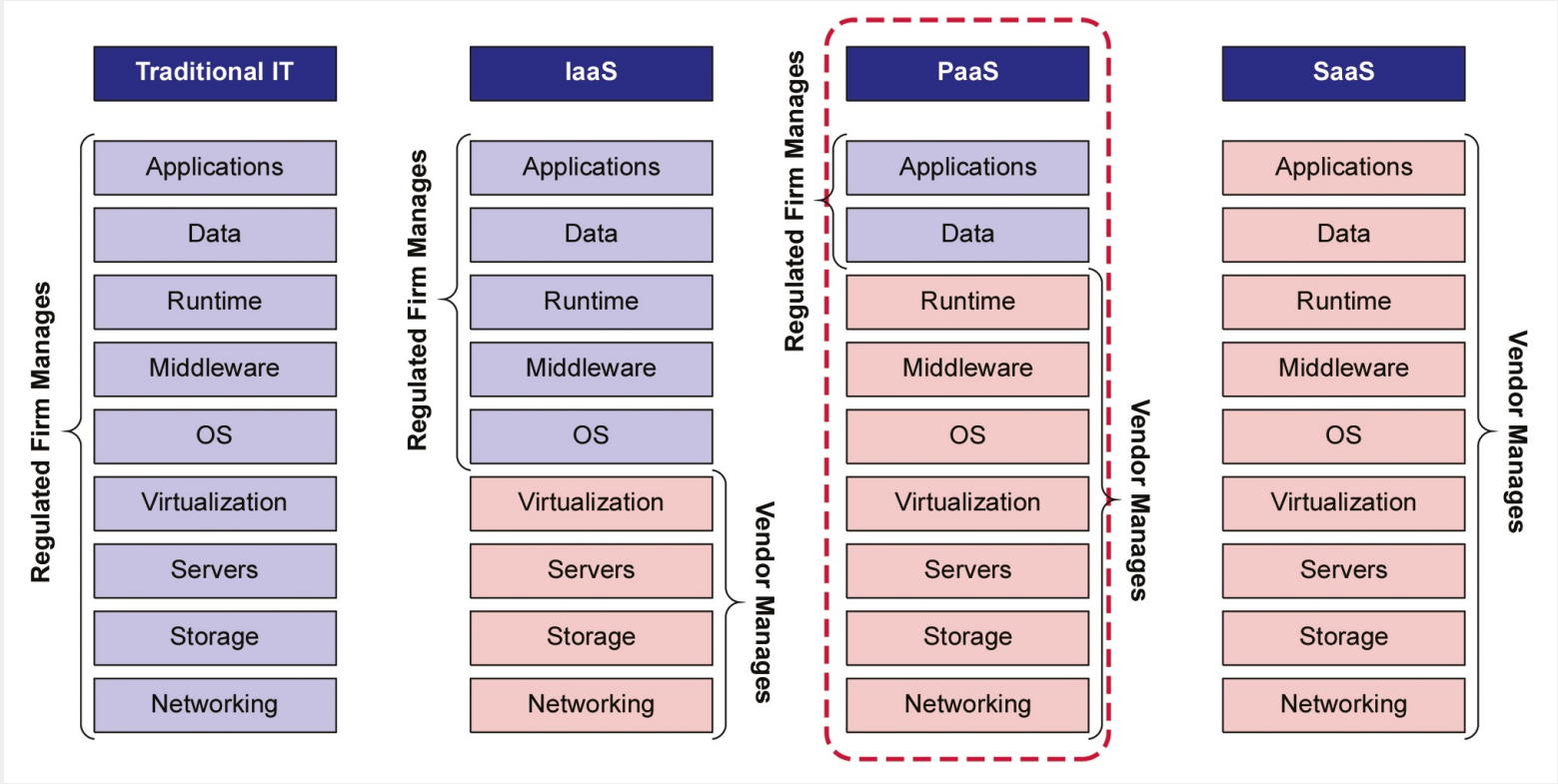
Forderungen an Cloud Service Provider (CSP)

digital chameleon

- Bekannte Marke/Reputation und Zertifizierungen/Audits (ISO 27001, NIST FedRamp, SOC) sind nicht ausreichend!
- **Kritische Anbieterauswahl mit Risikoabschätzung**
- **Durchführung von Lieferantenaudits bei CSP**
- **Anbieterauswahl immer anhand des Datenstroms/ Datenmodells sicherstellen**

Verantwortlichkeiten

- Verantwortlichkeiten prüfen und einfordern
- Quality Assurance Agreement (QAA) festlegen



IaaS Service Model vs Traditional IT Elements (Quelle: ISPE, 2014)

Audits & Vertragsmanagement

digital chameleon

- Überprüfung der Verträge (SLAs): Wer ist Data Owner? Was passiert mit Daten nach Kündigung?

  Backup & Restore Strategie, Access & Authorization durch CSP?

- Supplier Audit Fokus:
  - Management Systeme & Standards/Zertifikate
  - System Operations/Lifecycle Management (gelebt)
  - Service Management
  - Data Center
  - Architektur
  - IT Sicherheit
  - Datenschutz & Compliance

Beispiel: Fragebogen Supplier (Audit)

digital chameleon

CSV/ Software Lifecycle (System Acquisition, DEV & Maintenance) incl. Documentation	Compliance & Legal (auch GxP, Data Privacy/ Data Protection)	IT & Cyber Security Management (Cryptohraphy, Communication/Network, Security Incident)	Server Management (Data Center)	Access & Authentiification/ End-Point-Security beim Nutzer
Qualification & Testing/ Procurement, Installation and IQ	IT Architecture	Change Management incl. Risk Management	Configuration Management	Client Management
Network Management (Network Security, Transfer, Messaging)	Problem/ Incident Management	Help Desk provision	Record Management/ Backup, Restore, and Archiving	Disaster Recover & Business Continuity
Performance Monitoring	Supplier Relationsship Management /3rd party audits & controls	Periodic Review	Patch & Upgrade/ Release Management	

Beispiel: Verträge

digital chameleon

Quality Agreement – zur Einhaltung & Erfüllung von GxP, IT, Security & Privacy Standards
Data Ownership & Privacy/ Encrypt, remove, or redact data/ Beendigung & Löschung
Ausgebildetes Personal & Training
Rollen & Verantwortlichkeiten
Period Review & Evaluation beim Supplier
Audit Rechte einrichten lassen/ Service & Security Audits/ Sicherheitsprüfungen, Penetrationstests oder Schwachstellenanalysen
IQ & OQ verlangen (Platform Qualification)
Interne QA Involvement & Signature bei Qualification/ Testing, Risiko-Assessment & Aenderungen
Regelung bei Sicherheitsvor- fällen oder Betriebsunterbrechungen beim Cloud-Anbieter
Vertragsstrafen bei Nichterfüllung

WE ARE HAPPY TO SUPPORT YOU!

Digital Chameleon GmbH
Barfüsserplatz 3 | 4051 Basel |
Switzerland
Email: tanja.rohark@digital-chameleon.ch

digital chameleon