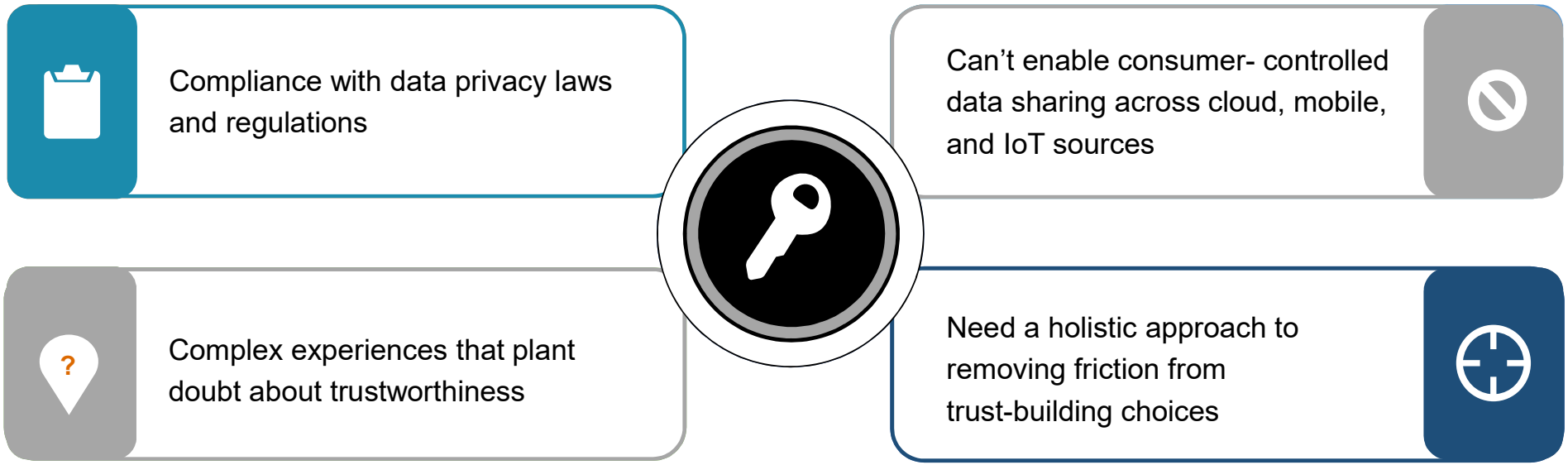
Building Trust through Privacy and Consent

Nick Caley
Vice President Industry
+44.7979.199549

FORGEROCK

Challenges in Handling Privacy and Consent



No More Data About You, Without You

GDPR Requirements

Consent	Right for access	Right to be forgotten
Privacy	Right to data portability	Right to Object
Notifications	Right to share	Right to delete

Privacy By Design

Controlling access to Personal Data for GDPR compliance

GDPR Articles 44-50	Implement fractional replication to control cross-border data transfers
GDPR Articles 25, 32	Implement variety of security and access controls to protect personal data
GDPR Articles 7, 33, 34, 83	Constrain access and identify erroneous login activity via audit data
GDPR Articles 5, 7, 12-23	Provide self-service, unified, and user-directed consent management
GDPR Article 5	Enable greater data accuracy through synchronization, API connections
GDPR Article 8	Protect children's data through managed identity workflows

Controlling access to Personal Data for GDPR compliance

- Use **global user profile** with a complete identity object, without a complete set of values everywhere
- **Fractionally replicate** a subset of attributes to jurisdictionally appropriate directory server instances
- **Filter personal data** from legacy application responses using gateway before arrival in an inappropriate jurisdiction
- For a user physically in a new jurisdiction, **route requests** using LDAP proxy or gateway for required session data unavailable in that jurisdiction's instance

Transfers of personal data to third countries or international organisations

Articles 44-50

- Enable **encryption, hashing, and tamper-proofing** at design time and run time, at all levels
- Enable contextual, adaptive **least-privilege access control mechanisms** to protect digital resources of all types
- Enable **IoT device protection**
- Deliver **end-user choice and control** for building trusted digital relationships

Data protection by design and by default; Security of processing

Articles 25, 32

Controlling access to Personal Data for GDPR compliance

- **Implement least-privilege access** through authorization and access control mechanisms
- **Contextual and fine-grained** authentication and authorization controls
- **Detect erroneous access** through audit logging service available in all components
- **Track** authentication methods, system access, user and admin activity, errors, and config changes
- Digitally sign for **tamper-evident logging**
- Consume log entries through many common **third-party SIEM and analytics** solutions
- Demonstrate **proof of consent** through audit logs

Personal data breaches; General conditions for imposing administrative fines

Articles 7, 33, 34, 83

- Provide **unified self-service interface** across many applications
- Enable **managing personal data** transparency and modification
- Enable **monitoring and managing consent** settings, including social sign-in and marketing automation API connections
- Enable **UMA sharing** transparency and control
- Enable **right to erasure** control
- Enable **right to data portability** control

Principles relating to processing of personal data; Conditions for consent; Rights of the data subject

Articles 5, 7, 12, 23

FORGEROCK

Thank You

FORGEROCK