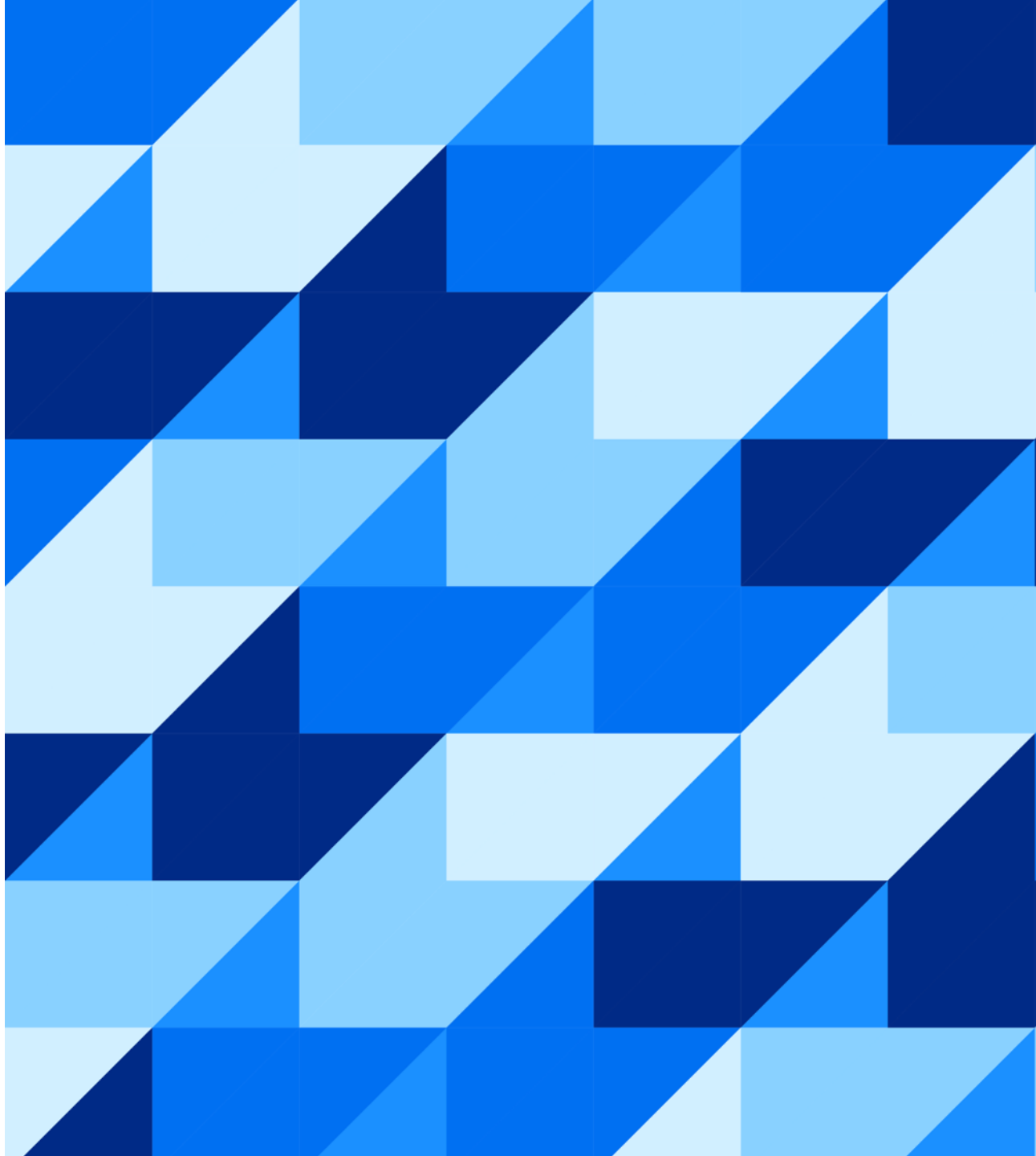
Data Protection in SAP S/4HANA (SAP Business Suite)

Processing and Safeguards

Volker Lehnert, SAP
Month 04, 2024



Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP’s intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Personal disclaimer

SAP does not provide legal advice, nor does the presenter.

The implementation of data protection requirements at any data controller is a complex challenge with interdependent legal and technical aspects. The responsibility to identify and implement adequate technical features remains with the controller as for the organizational aspects.

The following presentation is only about technical features which might in that sense help a controller achieving compliance with data protection regulations.

To help the audience understanding the shown approach, in context information is given without claiming completeness or correctness.

Agenda

Processing of personal data

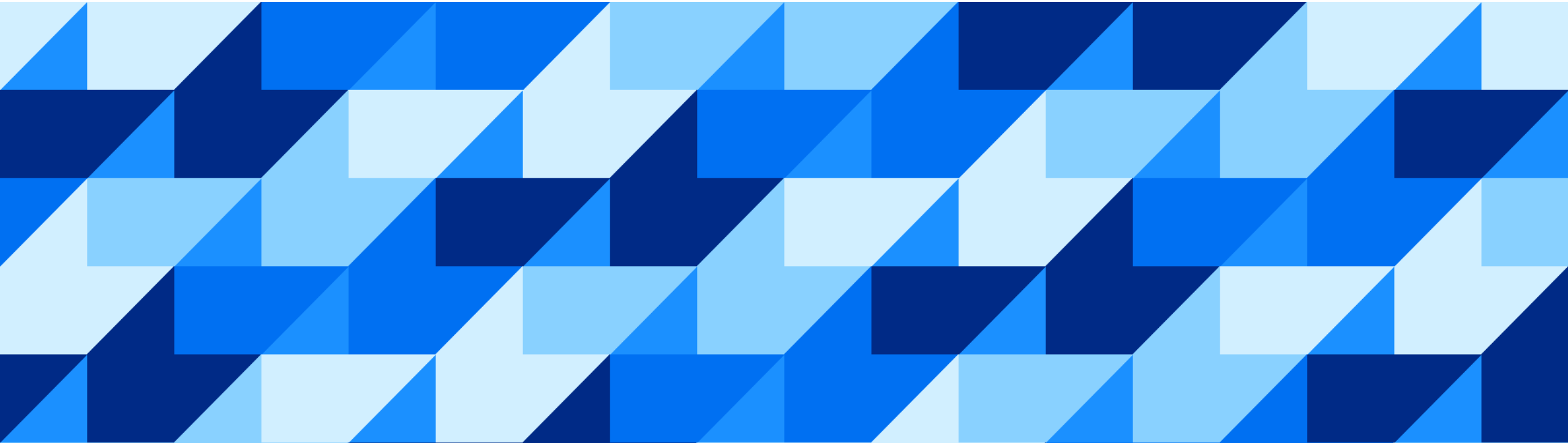
Self determination / Rights of the data subject

Security safeguards

Newest development

Outlook: Privacy by design and default: Purpose based!

Processing of personal data



Personal Data acc. to Art 4 No 1 GDPR

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal data acc. to The Digital Personal Data Protection Act (India) Art. 2

“(h) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means”

“(t) “personal data” means any data about an individual who is identifiable by or in relation to such data”

Personal Data acc. to Art 1 No. 4 KSA PDPL

Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

(Transl. SDAIA)

Personal data acc. to Art 2. 1. PIPA (Korea)

The term "personal information" means any of the following information relating to a living individual:

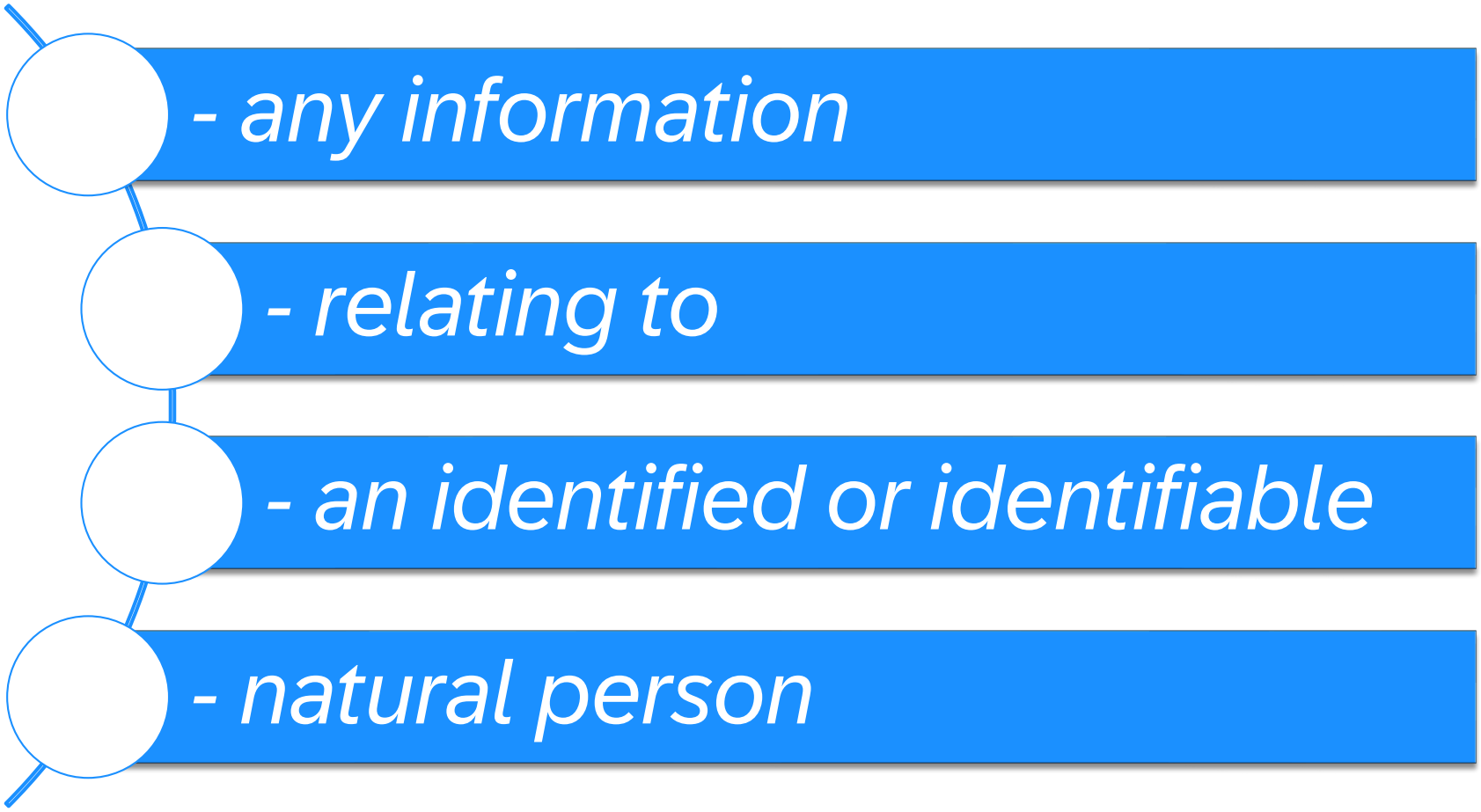
(a) Information that identifies a particular individual by his or her full name, resident registration number, image, etc.;
(b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. In such cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as likelihood that the other information can be procured;

(Translation KLRI / KLT)

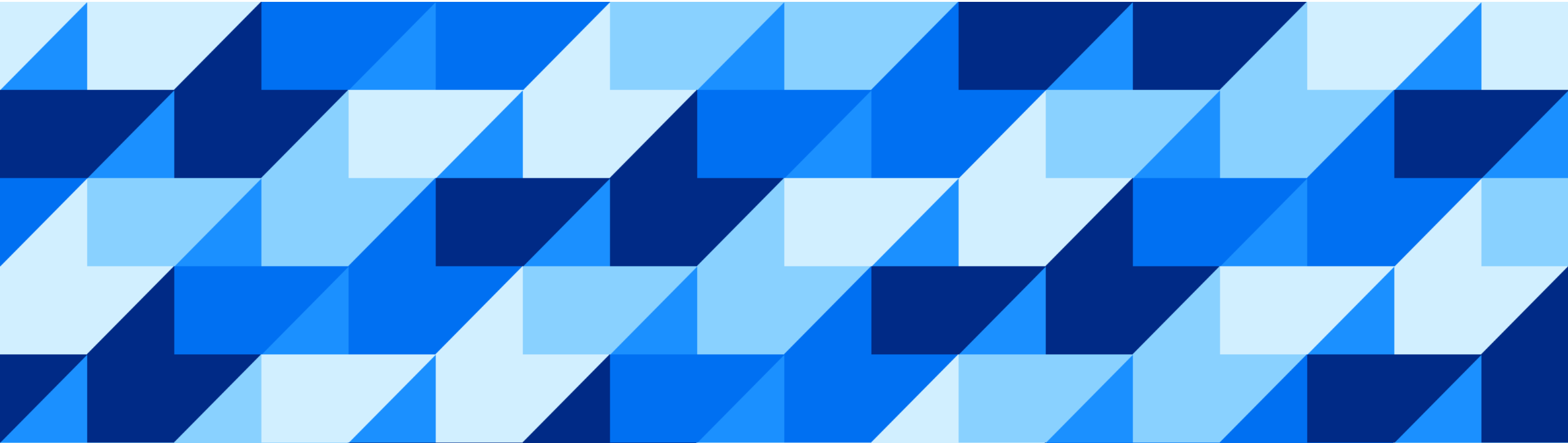
CPRA 1798-140 v (1)

(1) “Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: ....

The concept of personal data



Processing of personal data



Processing acc. to Art 4 No 2 GDPR

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processing acc. to The Digital Personal Data Protection Act (India) Art. 2

“(x) “processing” in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction”

Processing acc. to Art 1 No. 5 KSA PDPL

Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.

(Transl. SDAIA)

Processing acc. to Art 2. 2. PIPA (Korea)

The term “processing” means the collection, generation, connecting, interlocking, recording, storage, retention, value-added processing, editing, searching, output, correction, recovery, use, provision, disclosure, and destruction of personal information and other similar activities;

(Translation KLRI / KLT)

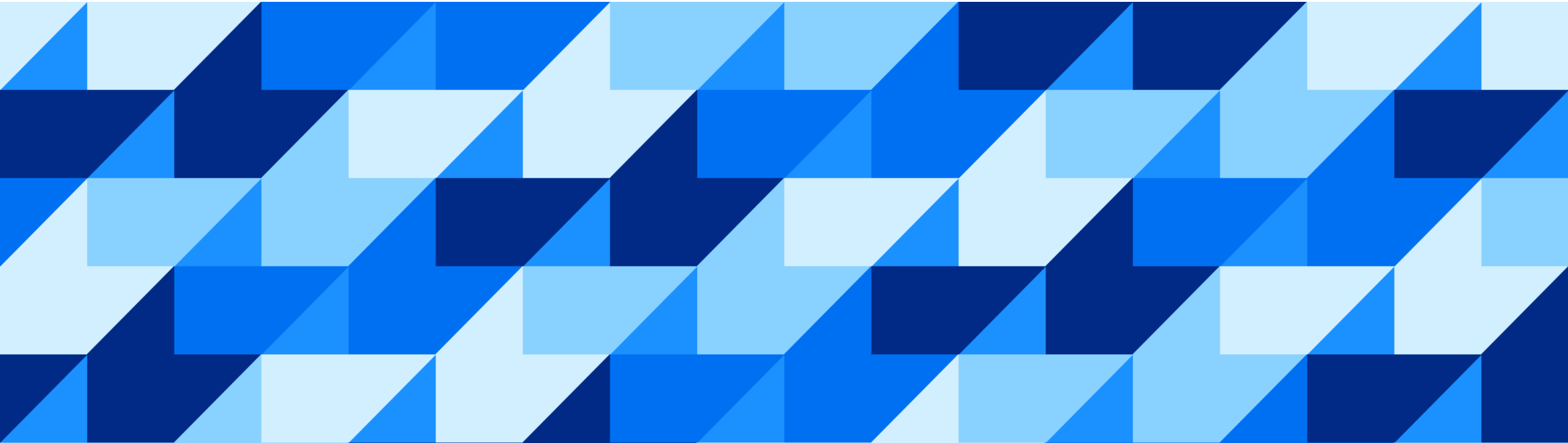
CPRA 1798-140 y

“Processing” means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

The concept of processing

... covers in an ERP system – simplified – any handling of personal data including storage, deletion, anonymization ...

Principles for processing of personal data



Processing of personal data

Legal basis

Processing of personal data

Considerations I – 1

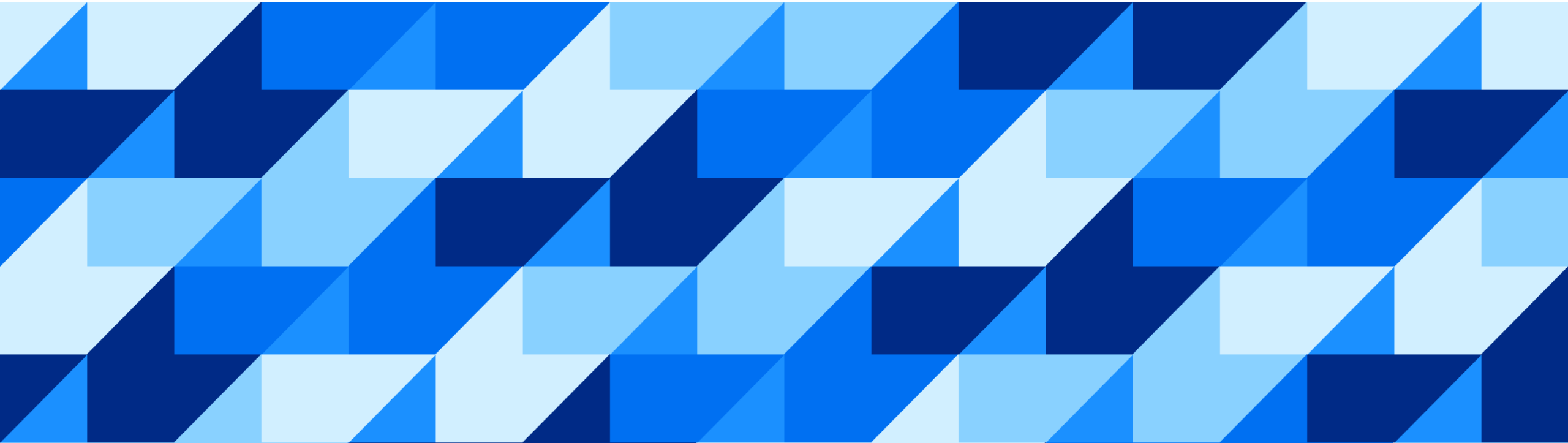
	Content	Possible Technical Feature?
Consent	Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. (GDPR rec. 42, sentence 1.)	Proof of consent is basically an organizational measure, however, the impact on data processing in an ERP system needs to be considered. • SAP Customer Data Platform offers a consent solution.
Contract	Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract. (GDPR rec. 44). More specific legislation might need to be considered. (example: as provided based on Art. 88 GDPR)	The proof of a contract is basically an organizational measure, however, an ERP system handles data documenting contracts: • The existence of a contract itself is documented by corresponding documents and postings. • As a supporting solution documentation in SAP GRC might be considered.
Legal Obligation	ERP based examples: tax reporting, income tax reporting, reporting for social insurance	The proof of a legal obligation is an organizational measure and not a technical feature. • As a supporting solution documentation in SAP GRC might be considered.

Processing of personal data

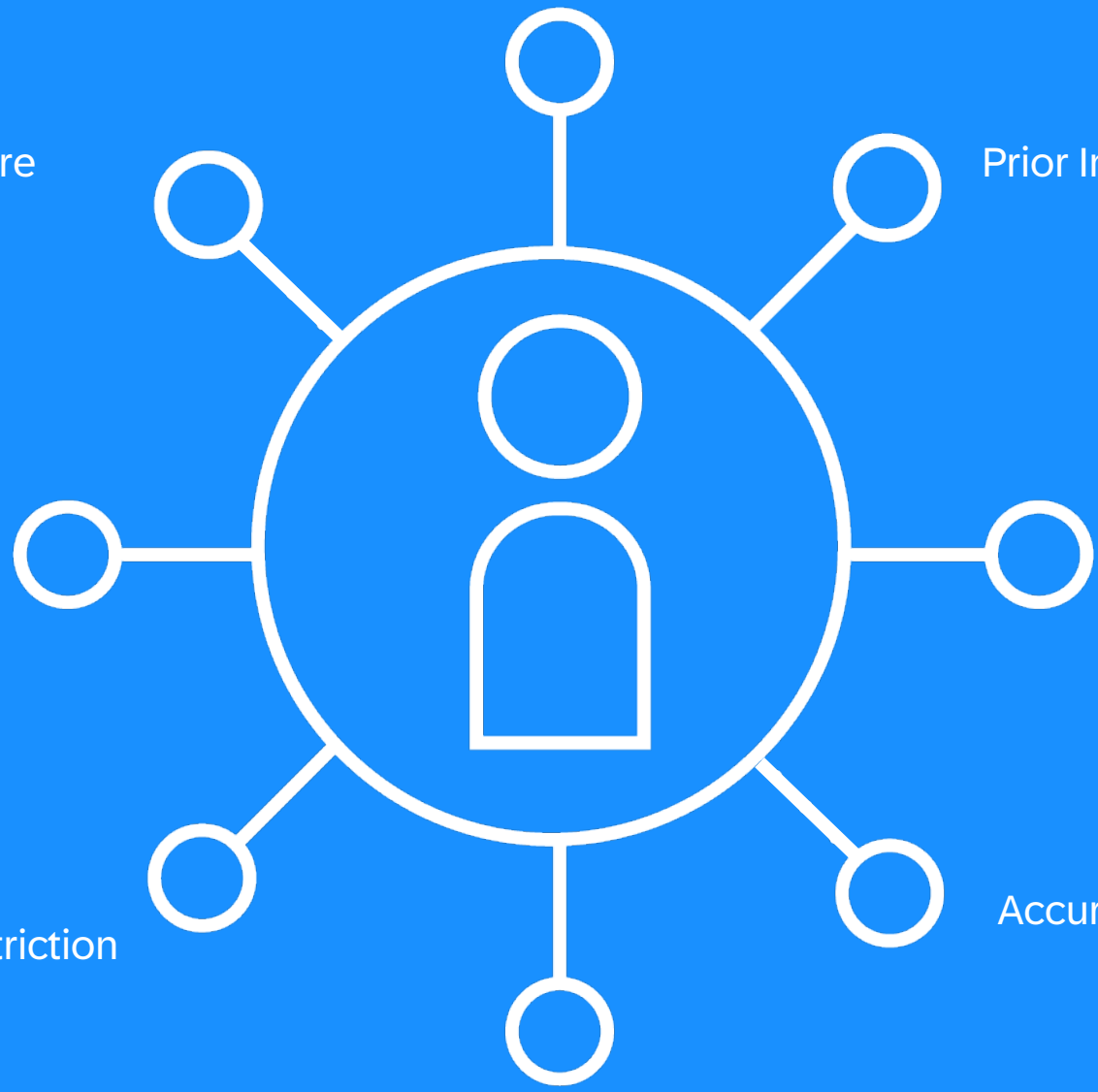
Considerations I – 2

	Content	Possible Technical Feature?
Protect Vital Interest	The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. (GDPR rec. 46 sentence 1)	The proof of a vital interest is an organizational measure and not a technical feature. • As a supporting solution documentation in SAP GRC might be considered.
Public Interest	Where processing is ... necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. (GDPR rec. 45 sentence 1)	The proof of a public interest is an organizational measure and not a technical feature. • As a supporting solution documentation in SAP GRC might be considered.
Legitimate Interest	Proofing a legitimate interest is subject to a careful legal consideration whether “fundamental rights and freedoms of the data subject” are not overriding such an interest. (GDPR rec. 47)	The proof of a legitimate interest is an organizational measure and not a technical feature. • As a supporting solution documentation in SAP GRC might be considered.

Self determination / Rights of the data subject



Self Determination / Data Subject Rights



SAP ILM Erasure

Prior Information (IRF)

IRF Portability

Information Access IRF

SAP ILM Restriction

Accuracy In Build

Automated Decision By design

Rights of the data subject

Considerations II – 1

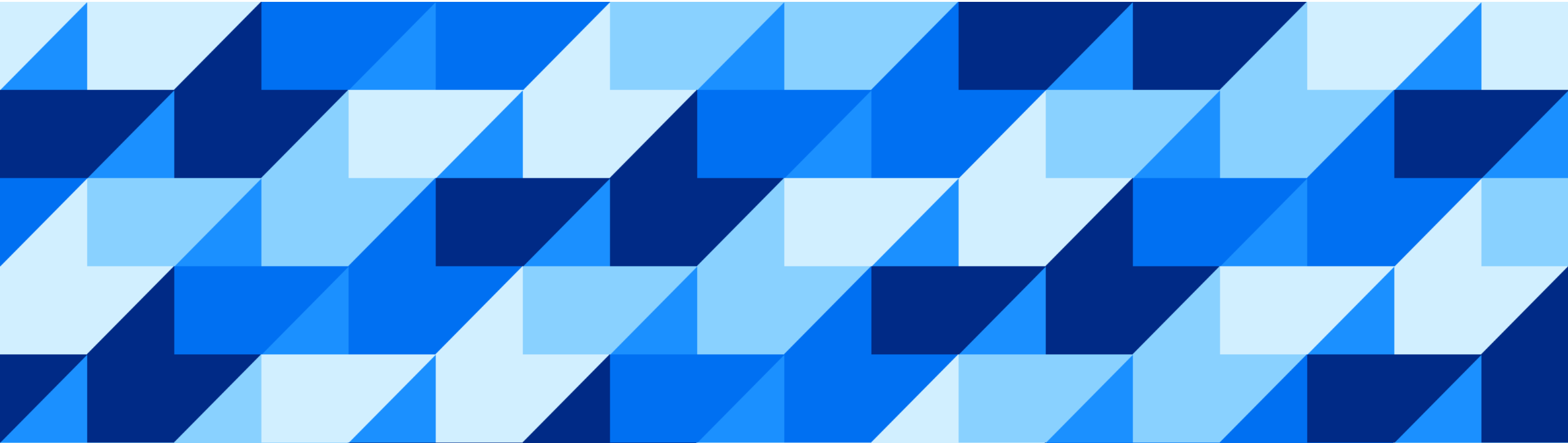
	Content	Possible Technical Feature?
Prior Information	Information to the data subject on the data undergoing processing, the data controller, the purpose, and the retention policies.	This information is an organizational measure and not a technical feature. • For SAP Business Suite and SAP S/4HANA an “Information Retrieval Framework” (IRF) is in implementation, that will support logically.
Information Access	The data subject’s right to get information on the data undergoing processing concerning them.	All personal data in SAP S/4HANA and SAP Business Suite is available for reporting in application specific reports. • For SAP Business Suite and SAP S/4HANA an “Information Retrieval Framework” (IRF) is in implementation.
Accuracy	Personal data has to be accurate, kept up to date and to be corrected (latest after request).	Correction is simple standard functionality. • Accuracy in terms of avoiding doublets and keeping up to date is supported from SAP MDG.
Erasure: Deletion/Blocking	The ability to delete personal data when all retention periods have passed. The ability to block personal data as soon as the primary purpose has passed and the residence time has elapsed.	SAP introduced based on SAP ILM the concept of the simplified blocking and deletion. • End of Purpose Checks, Blocking Indicators • Additional application specific procedures

Rights of the data subject

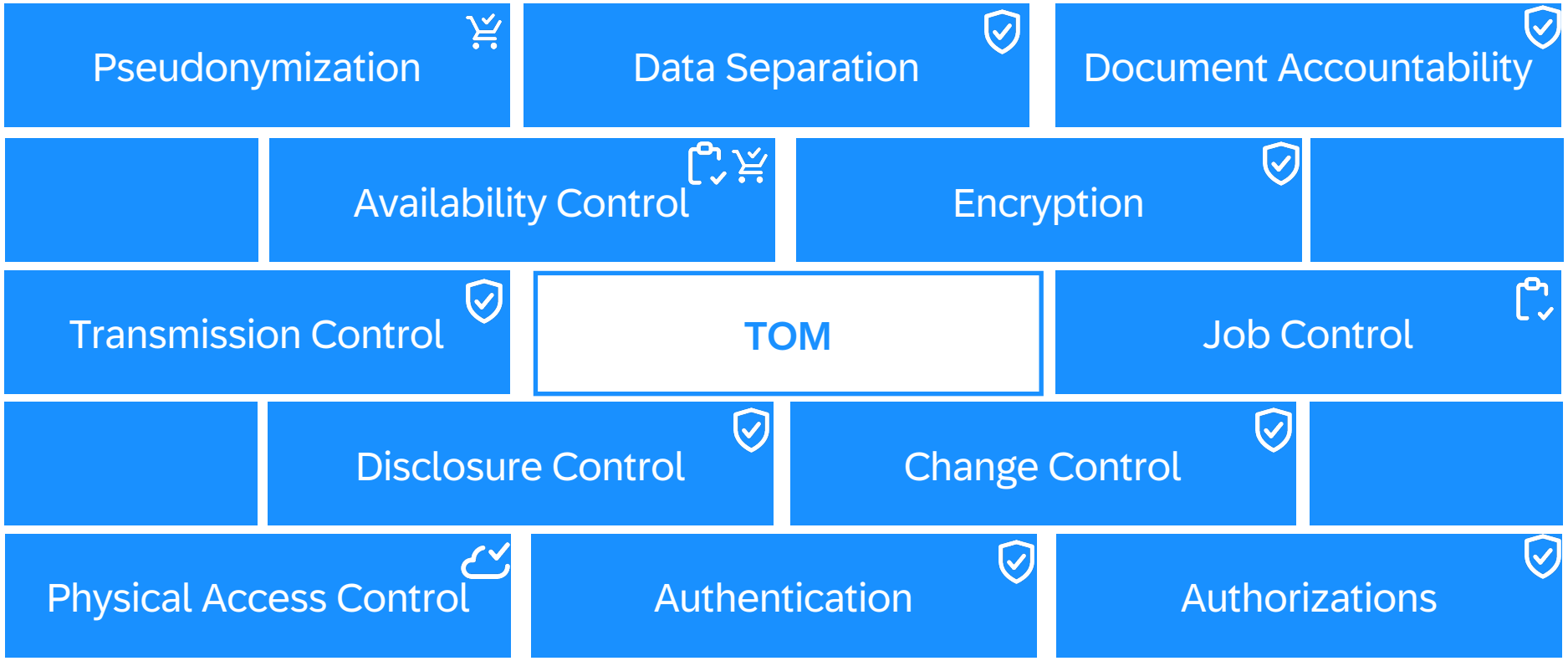
Considerations II – 2

	Content	Possible Technical Feature?
Portability	The right of the data subject to receive his personal data in a structured, commonly used and machine-readable format.	Most Information Access features provide download functionality. The challenges here are missing international standards and the complexity of personal data in business.
Restriction of Processing	The data subject has the right to obtain from the controller restriction of processing in certain cases	Subject to the Blocking and Deletion functionality
Automated Decisions	The data subject has the right, that any automated decision can become subject to manual interference.	Any features providing such capabilities are ensuring, that such decisions can get overruled manually.

Security safeguards



Safeguarding personal data



Build in
Part of contract
Cloud Obligation
Additional Service

Security safeguards

Considerations III – 1

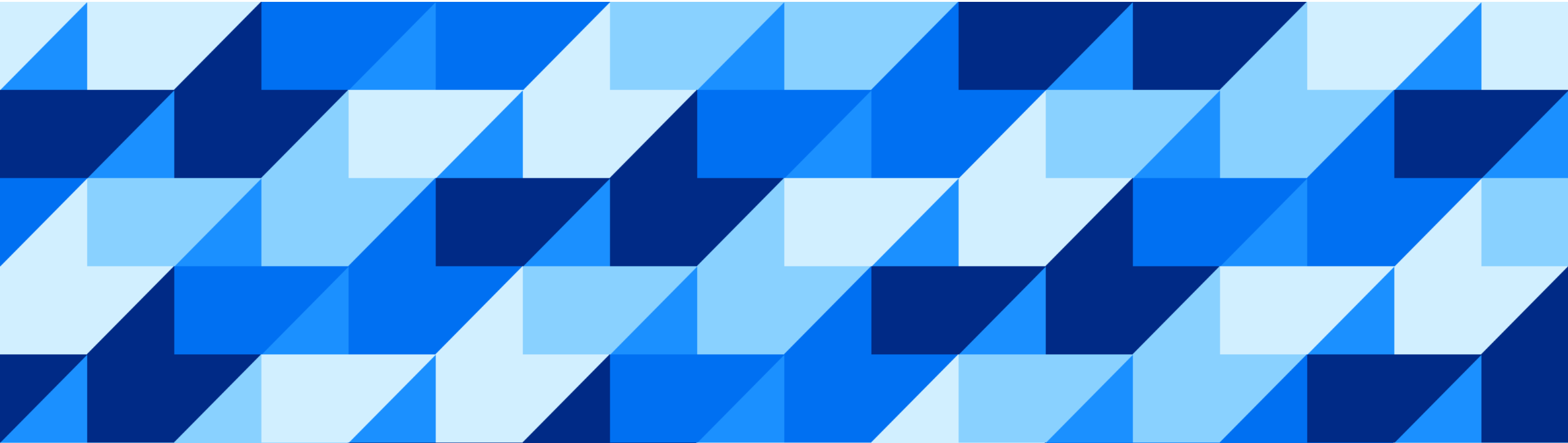
	Content	Possible Technical Feature?
Physical Access Control	Prevent unauthorized persons from gaining access to data processing systems with which personal data is processed or used	Such controls are not usually the subject of SAP Solutions. For example: Badges
Authentication	Secure procedures to enable system access based on personal authentication	Standard Authentication Features in SAP NetWeaver. • SAP SSO • SAP IDM
Authorization	Procedures allowing the differentiation of which data can be accessed and in which mode	Standard Authorization Concepts • SAP Access Control
Disclosure Control	Ability to document all access to personal data	SAP NW Tool Read Access Logging (RAL) available
Change Control	Ability to document all changes to personal data	Standard Change Logging

Security safeguards

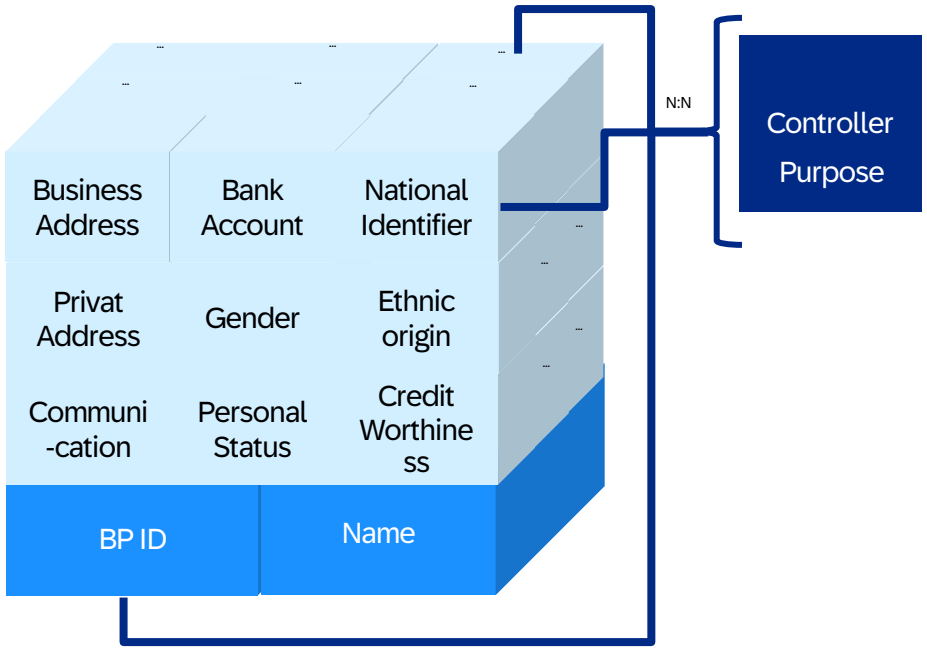
Considerations III – 2

	Content	Possible Technical Feature?
Transmission Control	Procedures and safe guards for the transmission of personal data, such as encryption during transmission	Standard features: RFC Security Encrypted communication • SAP ETD
Job Control	Data Controller has to ensure that the data processor is following his instructions and guidelines. This organizational task has some technical aspects like system audit	Standard System Audit • SAP GRC Suite
Availability Control	Procedures like back-up, disaster recovery, business continuity	Standard Features & Third Party
Data Separation	Personal data collected for a specified purpose must be separated from personal data collected for other purposes	Compliant Master Data Structures: • SAP MDG (Master Data Governance)

Newest development



Data Controller Assignment



Assignment of Data controller(s) to Business Partner

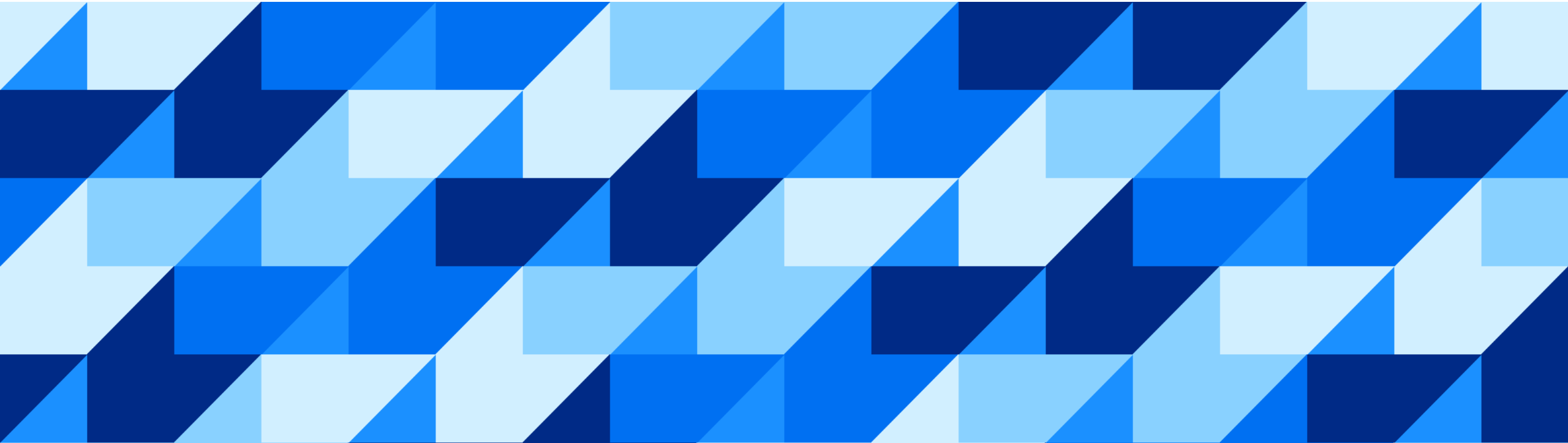
- Restrict access to this BP Object to the context of this / theses assigned data controller(s) only
- Assignment of additional data controller(s) allow access within the context of another data controller(s) (e.g. when a new data controller starts business with the BP)

→ When processing a BP in “data controller active” mode, all data controller processing this BP object must be assigned.

Assignment of Data controller(s) to transactional data

The existing line organizational attributes and authorizations on the level of transactional data are expected to be sufficient to separate data dependent on data controllers.

Outlook: Privacy by design and default: Purpose based!



Data Processing on Basis of Purpose

Data Separation: Purpose-based authorization checks for access by persons, machines, software logic.

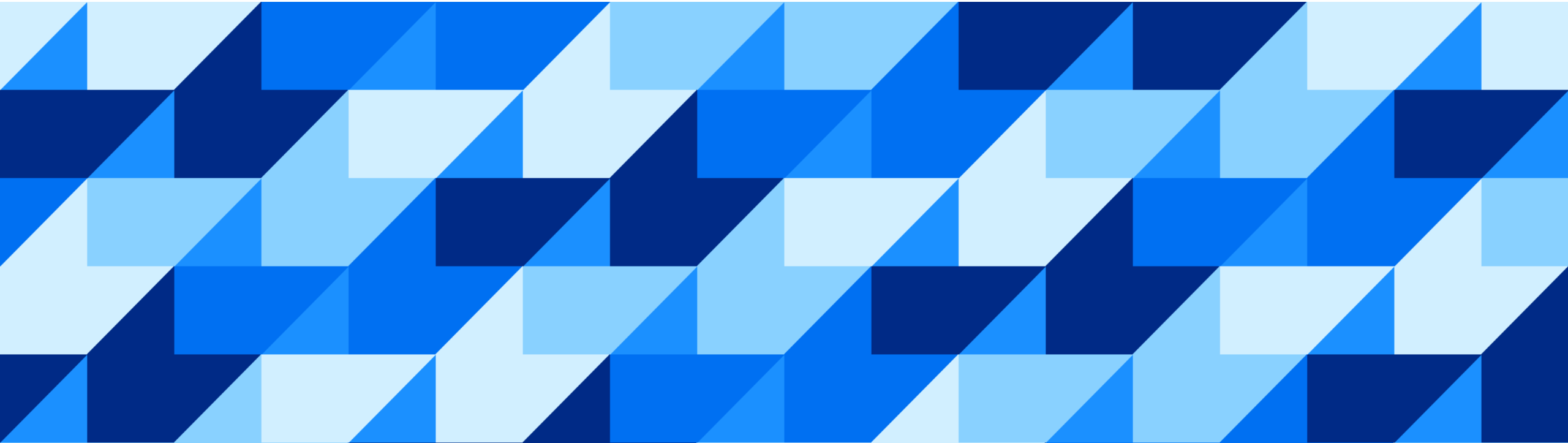
Once the primary purpose has ended:
Purpose based partial deletion, considering purpose related retention periods

Distribution to the systems:
Transmit only data relevant based on purpose of data processing in target system.

Provide data subject with information on all his/ her data structured by purpose

+ For any operation, you need to **document based on which purposes data is being processed:** ROPA, PIA, TOM.

Links



Further information

SAP public

How SAP is implementing the requirements of the General Data Protection Regulation (GDPR) to best support its customers
https://www.sap.com/about/cloud-trust-center/data-ownership-privacy.html#pdf-asset=84d6bf89-bb7c-0010-82c7-eda71af511fa&pdf-page=1
Part 2: Product and Services Compliance – https://www.sap.com/about/cloud-trust-center/data-ownership-privacy.html#pdf-asset=9a35c37d-cc7c-0010-82c7-eda71af511fa&pdf-page=1
SAP Integrated Report 2016 – Governance – Security, Privacy, and Data Protection https://www.sap.com/integrated-reports/2016/en/governance/security-and-privacy.html

References

GDPR and SAP - Data Privacy with SAP Business Suite and SAP S/4HANA (Lehnert/Luther/Pluder/Christoph/ Fernandes)
https://www.rheinwerk-verlag.de/gdpr-and-sap_4652/
Datenschutz mit SAP (Lehnert/Luther/Pluder/Christoph)
https://www.rheinwerk-verlag.de/datenschutz-mit-sap_4524/
Meeting Modern Data Protection Requirements - How SAP Business Suite Helps You Comply with GDPR (Volker Lehnert)
http://sapinsider.wispubs.com/Assets/Articles/2017/August/SPI-Meeting-Modern-Data-Protection-Requirements
Datenschutzanforderungen und ihre Unterstützung in HR-Systemen am Beispiel SAP ERP HCM (Lehnert/Dopfer-Hirth)
HMD Praxis der Wirtschaftsinformatik.
Vereinfachtes Sperren und Löschen personenbezogener Daten in der SAP Business Suite (Lehnert/Pluder)
www.datenschutz-berater.de Nr. 10/2016
SAP-Berechtigungswesen (Lehnert/Stelzner/Otto/John)
https://www.rheinwerk-verlag.de/sap-berechtigungswesen_3849/

Thank you.

Contact information:

Volker Lehnert, Senior Director Data Protection S/4HANA
volker.lehnert@sap.com

Headline with divided text – two columns

H**eadline**

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

H**eadline**

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Headline with divided text – two columns

H**eadline**

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

H**eadline**

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Body text goes here, and can run to several lines or more

Table – eight columns

Label 1	Label 2	Label 3	Label 4	Label 5	Label 6	Label 7	Label 8
Category	123	123	123	123	123	123	123
Category	123	123	123	123	123	123	123
Category	123	123	123	123	123	123	123
Category	123	123	123	123	123	123	123
Category	123	123	123	123	123	123	123
Category	123	123	123	123	123	123	123