KST LAW

New guidelines on personal data protection in the payment and e-money sector

On 11 April 2025, the Turkish Data Protection Authority ("**DPA**") and the Turkish Payment and Electronic Money Institutions Association released the Best Practices Guidelines on the Protection of Personal Data in the Payment and Electronic Money Sector ("**Guidelines**").

This is the first set of sector-specific guidance in Türkiye addressing how personal data should be processed within the payment and e-money ecosystem. The Guidelines serve as a practical tool for data controllers and data processors to ensure compliance with Turkish Law No. 6698 on the Protection of Personal Data (the "**DP Law**").
The Guidelines provide in-depth insight into several key topics, including:

1. Core service areas and how personal data is processed

The Guidelines identify five core service areas in the payment and e-money sector, explaining the related personal data processing activities:

i. **Electronic money issuance:** Defined under Law No. 6493[1], this refers to the issuance of a monetary value used in payment services. Although it enables transactions, it is not classified as a payment service itself.

ii. **Money remittance:** A service where funds are transferred between individuals without requiring a payment account.

iii. **POS services:** Point-of-sale systems enabling card-based payments operated through collaboration between banks and payment institutions. The transaction is instantly processed through the banking data system, enabling collection from the cardholder.

iv. **Bill payment intermediation:** A service allowing users to pay utility bills (e.g., electricity, water, gas, and telecommunication) via a payment service provider.

v. **Mobile payment:** This service enables transactions via mobile phone lines, where mobile operator shares the phone number with the payment service provider to complete the transaction.

2. Who's who in the data ecosystem: Data controller, data processor, and data subject roles

The Guidelines clarify the roles of data controllers, data processors, and data subjects for each core services in line with the DP Law and Law No 6493.

Core Service	Data Controllers	Data Subject
Electronic money issuance	▪ Electronic money institutions	Individuals: ▪ benefiting as electronic money users ▪ acting as sender/recipient during the transfer of electronic money ▪ using money remittance services as sender/ recipient ▪ who are customers of the payment institution providing POS services ▪ who own individual mobile lines and benefit from mobile payment services ▪ acting as representatives of legal entities and individual beneficiaries of payment and e-money services
Money remittance	▪ Payment institutions of sender & recipient	
POS services	▪ Payment institutions providing POS services ▪ Merchants ▪ Banks	
Bill payment intermediation	▪ Payment institution providing Bill payment service	
Mobile payments	▪ Mobile operators ▪ Payment institutions affiliated with the mobile operator ▪ Merchants	
Data Processors		
Representatives of institutions, service providers, and those offering secondary services (e.g., IT, marketing, customer support) may act as data processors, depending on their role and activities.		

The Guidelines emphasise the joint responsibility between data controllers and processors to safeguard personal data and ensure compliance with technical and organisational measures under the DP Law.

In addition, the Guidelines emphasise the ongoing legal responsibilities of data controllers under the DP Law. These include:

- informing data subjects about their data processing activities;
- registering with the Turkish Data Controllers' Registry System (**VERBIS**);
- complying with other statutory obligations, such as data security and retention rules, data breach incident procedures, etc.

[1] Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions No.6493

3. Practical examples: When is an entity a data controller?

The Guidelines provide practical examples of data controller roles in specific payment-related scenarios:

QR code fuel payment: When a customer pays for fuel using a QR code, the payment institution is considered the data controller for the personal data processed during the transaction.

E-commerce payment transactions: When a customer completes a purchase on an e-commerce website and enters payment information via the site's integrated payment screen, both the payment institution and the e-commerce platform (transferring the card data) are considered data controllers for the respective stages of data processing.

Bill payment intermediation: In bill payment services, transactions are often handled by authorised representatives of the payment institution (e.g., physical branches). In this structure, the payment institution remains the data controller for the personal data of the customer making the payment, while the representative, acting on its behalf, serves as the data processor.

4. Categories of personal data processed

The Guidelines include examples of various categories of personal data processed in the payment and e-money sector, depending on the nature of the service provided:

Core Service	Examples of Categories of Personal Data Processed
Electronic money issuance	Identity, contact, financial information, professional and educational information, transaction security information, visual and audio records, biometric data
Money remittance	Identity, contact, educational information
POS services	Identity, contact, transaction security information, customer transaction, financial information, visual and audio records, biometric data
Bill payment intermediation	Identity, contact, transaction security information, customer transaction
Mobile payment	Identity, contact, subscription, financial information, risk information, transaction security information, customer transaction

5. General principles and lawful bases for processing personal data

The Guidelines emphasise that personal data processing activities must comply with the general principles set out under the DP Law: lawfulness, fairness, accuracy, purpose, data minimisation, and storage limitation.

The Guidelines provide several lawful bases under DP Law for processing personal data in the payment and e-money sector. Key examples are summarised in the table below:

Legal Basis under the DP Law	Examples of Personal Data Processing
Explicit consent	▪ Sending commercial e-messages based on personal data obtained during the provision of payment services. ▪ Using customer data collected through POS services for marketing activities or profit-enhancing purposes. ▪ Collecting and processing biometric data (e.g., facial recognition, fingerprint) during identity verification.
Statutory requirement	▪ Processing identity information to meet customer identification requirements, as expressly required by applicable laws.
Contractual necessity	▪ Processing personal data to complete the payment between a merchant and customer as part of the underlying sales/service contract.
Legal obligation of the data controller	▪ Processing personal data to comply with obligations under relevant legislation (e.g., identification and storage requirements, anti-fraud measures).
Establishment, exercise, or protection of a legal right	▪ Submitting personal data as part of legal proceedings to fulfil the burden of proof.
Legitimate interests of the data controller	▪ Analysing transaction data to detect unusual or suspicious activities by payment services users, provided such interest does not override the data subject's fundamental rights.

6. When and how Is cross-border data transfer lawful in the payment sector?

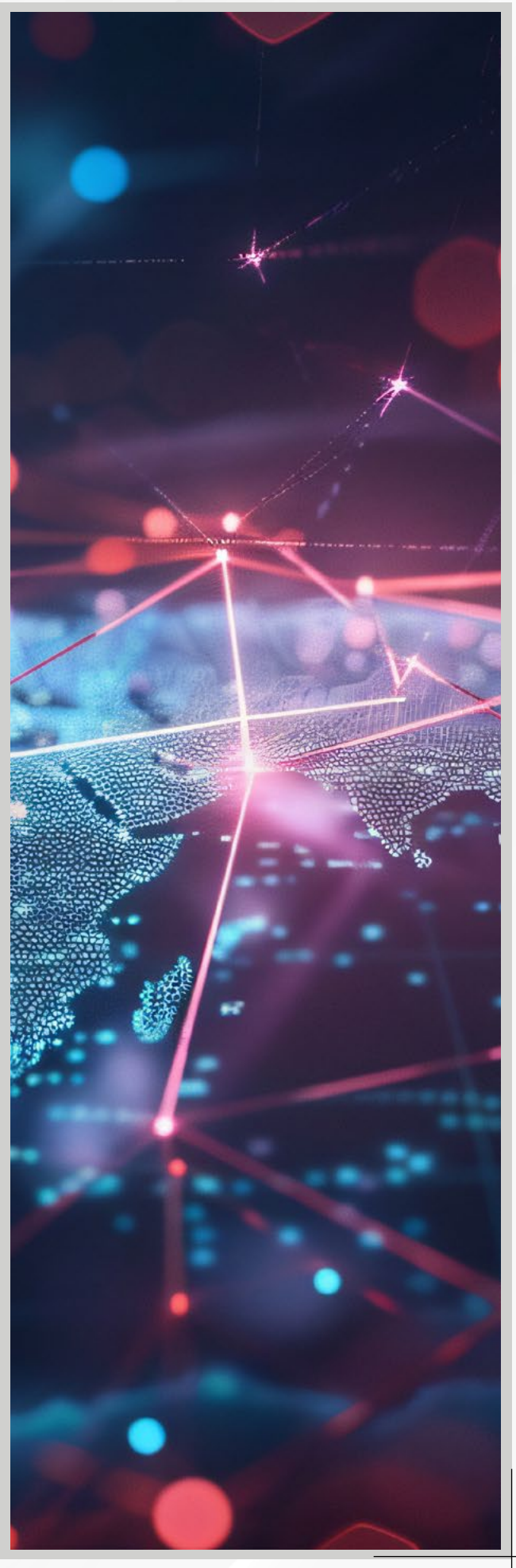
When personal data is transferred abroad, both Article 9 of the DP Law and sector-specific regulations applicable to the payment and e-money sector must be considered. In particular, Law No. 6493 imposes a local data storage requirement, meaning institutions in this sector are required to store certain data within Türkiye. Accordingly, they must ensure compliance not only with the general principles of the DP Law, but also with sector-specific obligations concerning data residency.

As highlighted in the Guidelines, one common scenario involves international money remittance transactions. If such a transfer is considered "occasional" and is necessary for the performance of a contract between the data subject and the data controller, it may be carried out without explicit consent and additional safeguards, in line with Article 9 of the DP Law.

In conclusion

The Guidelines represent a significant development for the payment and e-money sector in Türkiye, when personal data is processed continuously and intensively. All institutions in the payment and e-money sector must take necessary steps to ensure full compliance with the DP Law.

You can access the full text of the Guidelines (in Turkish) **here**.



KST LAW

We provide legal services relevant to all aspects of business in a wide variety of sectors, in particular focusing on mergers and acquisitions, commercial and financing transactions, dispute resolution as well as general corporate and regulatory advice.

Contact Us:

Ceren Ceyhan
ceren.ceyhan@ksthukuk.com

Hatice Nur Arslan
nur.arslan@ksthukuk.com