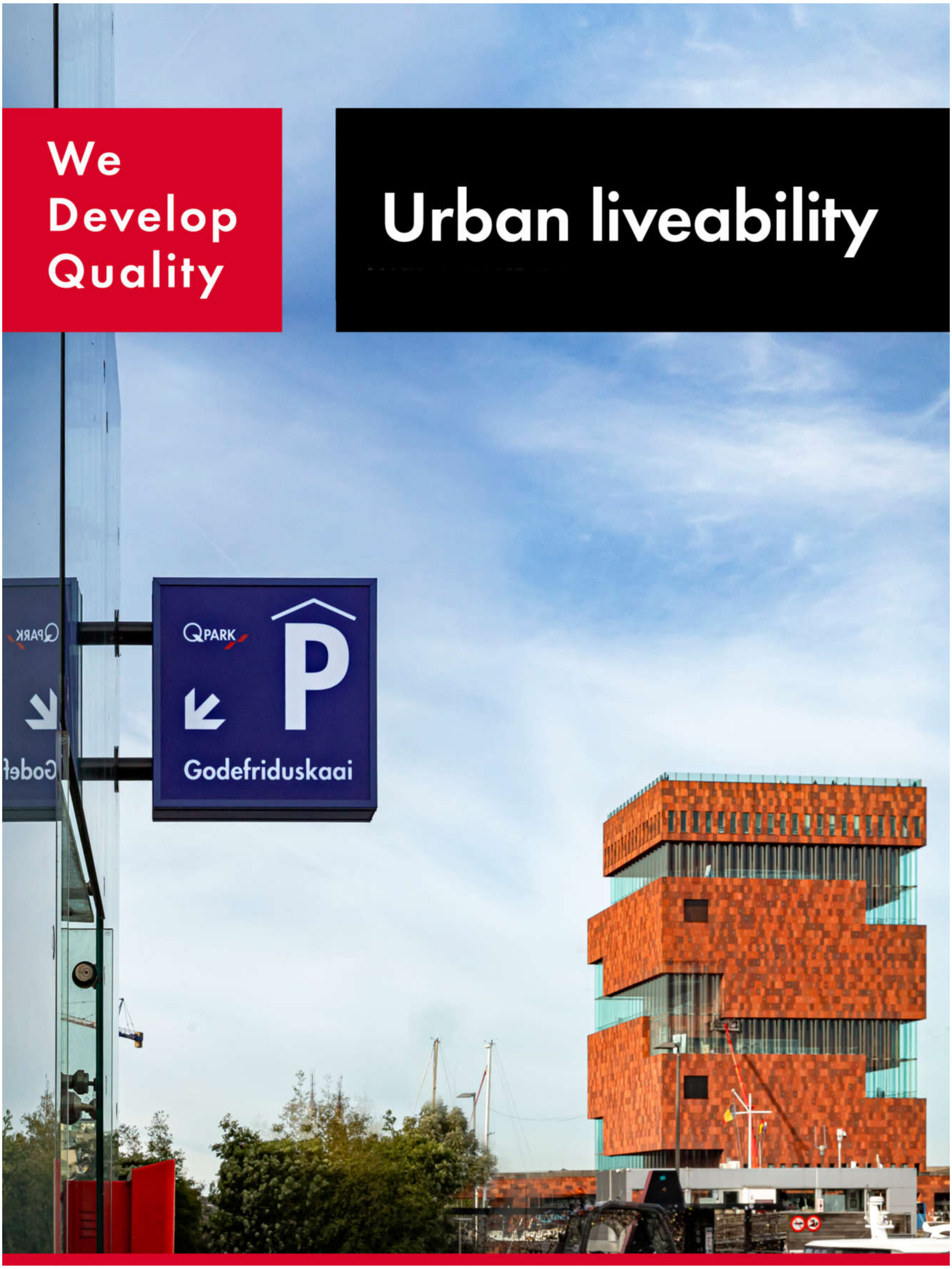
ANNUAL CSR REPORT 2023



We Develop Quality

Urban liveability

Q-PARK Quality in parking

GOVERNANCE

Good governance includes risk management and compliance to regulations and legislation as well as proper supplier relationship management and policies to counter corruption and bribery.

Compliance

Compliance for continuity

Compliance is important to any organisation and at Q-Park we take all aspects of compliance seriously.

- Our compliance programme covers the most relevant compliance areas for Q-Park. It helps us structure our approach to compliance and is therefore designed to minimise risks to the continuity of our business.
- Our compliance programme ensures that actions taken as part of the risk control cycle are performed based on a clearly defined plan with clear roles and responsibilities.

Compliance focus areas

Our priority compliance focus areas are:

- Information security, including PCI DSS
- Ethics and Integrity
- Employment and pensions policy
- Tax, per country and at corporate level
- GDPR
- Risk Control framework

Information security

Information security receives special attention

As part of our compliance programme we have established a multi-year Cybersecurity Training and Awareness Programme for employees.

During 2023 we have had one personal data breach as we disclosed e-mail addresses by mistake when informing a select group of season ticket holders about the accessibility of a specific parking facility.

Ethics and integrity

We have the Q-Park Integrity Policy and Trade Sanctions Policy in place. A training and awareness programme is scheduled every two years to raise awareness of the importance of this compliance area and to make improvement actions sustainable.

Click here for our Integrity Policy.

Click here for our Trade Sanctions Policy.

Governance, policies and codes

All static information regarding Q-Park governance, policies and codes can be found on our corporate website as this information does not depend on the reporting year.

Click here for our Corporate governance.

Click here for our Integrity Policy.

Click here for our CSR Code.

HRM Portal

All employees have access to our HRM Portal. This is where they can access all relevant HRM services and can find information about their salary, holiday entitlements, benefits and pension as well as their training programme.

We also publish our policies in the HRM Portal, this means employees always have access the latest versions of the:

- Equal treatment and opportunities for all
- Working conditions
- Pensions policy
- Whistleblower policy
- Integrity policy

Risk management

A business must take risks to create value. Having a risk management assessment in place allows a company to take risks in a managed and controlled manner. Strategic, operational, financial, and reputational risks are made manageable by carefully weighing risks and returns against each other. Effective risk management is integrated into our daily operations.

Q-Park deploys a top-down risk management assessment in which strategic risk management is executed at corporate level. Responsibility for operational risk management lies primarily with local country management. The Management Board and key management bear ultimate responsibility for managing the risks the Group faces.

Risk management and internal control

Ongoing identification and assessment of risks is part of our governance and periodic business review. Our Enterprise Risk Management (ERM) assessment and Compliance Programme are designed to provide management with an understanding of the key business risks. These also provide methods and processes to manage risks that might hamper the business in delivering on our strategy.

Q-Park is averse to the risk of non-compliance with relevant laws and regulations, our own codes, contractual agreements and financial covenants. As legislation and other formal guidelines cover various functional areas and can be very extensive (even country specific), we manage compliance in a structured way. Our Compliance Programme covers most relevant compliance areas for Q-Park, ensuring:

- the tone at the top regarding the importance of compliance;
- that the actions per step of the risk control cycle are executed based on a clearly defined plan with clear roles and responsibilities;
- that implementation of relevant legislation and internal guidelines within the organisation is assured.

The Management Board and key management periodically review the risks and related mitigation controls and procedures of the ERM assessment and our Compliance Programme, and reconsider the identified focus areas. Furthermore, they provide complementary insights into existing and emerging risks that are subsequently included in the policy. The ERM assessment and Compliance Programme determine the formation of controls and procedures, as well as the focus of business planning and performance process.

In 2023, the most significant developments in risk focus areas centred on:

- Monitoring our financial structure in light of economic circumstances and the Group's performance while preparing for refinancing the issued 2025 notes. Preparations for the refinancing were completed in December 2023 and the actual refinancing was executed in January 2024 as also disclosed in note 14 'Events after balance sheet date' of the annual accounts.
- Further implementation of the information security programme which covers 'people', 'process' and 'technology' angles to bring our information security maturity to a higher level. After consolidating our ICT infrastructure (hosting platform, connectivity platform, end-user equipment), ICT organisation and processes, we shifted focus towards proactive end-to-end security so we can better anticipate, identify, protect, detect and respond to threats and vulnerabilities. As part of this approach, we identified three priority tracks which were further rolled out in 2023 and will continue into 2024:
  - **Asset Management**: to monitor relevant information security aspects of assets attached to our network;
  - **Segmentation**: to be able to isolate parking facilities in our network in the event of a security incident (e.g. malware infections);
  - **Security awareness**: to improve employee awareness regarding cyber and information security by continuous