DTEC

Legal Memorandum

GDPR Compliance Assessment for DTEC's Website and Corporate Documentation

23.06.2025 (v1.0)

vircon
LEGAL CONSULTANCY

GDPR Compliance Assessment for DTEC's Website and Corporate Documentation

Subject: Legal Memorandum on the Assessment of the DTEC Platform and Website in Light of GDPR Compliance Requirements

EXECUTIVE SUMMARY

This memorandum provides a comprehensive review of DTEC's data protection practices in relation to its website (https://dtec.space/), API-based connected vehicle platform, and associated operational workflows. The aim is to determine the current level of compliance with the EU General Data Protection Regulation (GDPR) and to identify gaps or areas for improvement.

Key findings include:

- Partial compliance with transparency and data subject rights obligations.
- Absence of cookie management mechanisms in line with the ePrivacy Directive.
- Insufficient disclosures on lawful basis, third-country transfers, and data minimization.
- Need for a DPIA due to large-scale processing and use of sensitive data.

To move toward full compliance, DTEC is advised to implement a Consent Management System (CMS), update its Privacy Policy to reflect GDPR requirements, and introduce appropriate legal and technical safeguards for data processing involving blockchain and vehicle-linked identifiers.

These steps will help ensure regulatory compliance, improve user transparency, and position the platform for responsible growth within privacy-sensitive markets.

TABLE OF CONTENTS

1. INTRODUCTION

DTEC, a financial technology company based in Amsterdam, operates a connected vehicle API platform integrating blockchain-based functionalities and voice-assisted data collection (DtecA). As a data controller and processor under GDPR, DTEC must ensure that all personal data processing activities—including those via its website and developer-facing services—are conducted in full compliance with GDPR requirements.

This memorandum evaluates DTEC's compliance with GDPR and related data privacy obligations. It includes both a legal and operational assessment of its platform and associated documentation, with practical recommendations for achieving full compliance.

2. LEGAL FRAMEWORK

The processing of personal data by DTEC through its website, mobile applications, APIs, and blockchain infrastructure is primarily governed by the following legal instruments and regulatory frameworks:

a. General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

As DTEC is established in the Netherlands and targets data subjects within the European Economic Area (EEA), it is directly subject to the GDPR. The GDPR imposes comprehensive obligations on data controllers and processors, including, but not limited to:

•Lawful basis for processing personal data (Art. 6),

•Transparency and information obligations (Art. 13–14),

•Data subject rights (Art. 15–22),

•Data protection by design and by default (Art. 25),

•Security of processing (Art. 32),

•Records of processing activities (Art. 30),

•Data Protection Impact Assessment (Art. 35),

•International data transfers (Chapter V),

•Joint controllership and third-party processor obligations (Art. 26, 28),

•Consent management, where applicable (Art. 7).

b. ePrivacy Directive (Directive 2002/58/EC, as amended by Directive 2009/136/EC)

To the extent that DTEC uses cookies, trackers, or similar technologies on its website, the provisions of the ePrivacy Directive (as implemented by Dutch Telecommunications Act) apply. This includes obligations regarding:

•Prior consent for non-essential cookies,

•Clear and comprehensive cookie notices,

•Opt-out mechanisms for behavioral advertising and analytics tools.

c. Dutch Implementation of GDPR: Algemene Verordening Gegevensbescherming (UAVG)

The Dutch GDPR Implementation Act (UAVG) supplements the GDPR with national provisions, including:

•Specific rules on processing biometric or health-related data (if applicable through in-vehicle sensors),

•Enforcement powers of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens),

•National rules on data processing for scientific, statistical, or historical research purposes.

d. Blockchain-Specific Considerations under GDPR

Given that DTEC utilizes blockchain technology for recording certain data transactions, the immutable and decentralized nature of blockchain must be evaluated against GDPR principles, especially:

•Compliance with the data minimization and storage limitation principles (Art. 5),

•Exercising data subject rights such as rectification or erasure (right to be forgotten),

•Definition of controllership in a decentralized context (whether DTEC remains a sole controller, joint controller, or part of a larger ecosystem),

•Tokenization, anonymization, and pseudonymization measures,

•Safeguards for linking blockchain addresses to identifiable users.

e. Cybersecurity Frameworks and Consumer Protection (Supplementary)

While not specific to personal data, DTEC must also consider broader legal instruments such as:

•The EU Cybersecurity Act (Regulation (EU) 2019/881) for trust and transparency in digital infrastructure,

•Consumer protection rules (e.g., misleading practices, digital service quality),

•Digital Services Act (DSA) and Digital Markets Act (DMA) if the Platform qualifies under their scope in the future.

3. LEGAL ASSESSMENT

As part of this memorandum, the DTEC website, Privacy Policy, user interface elements, and related documentation were reviewed to assess their compliance with the General Data Protection Regulation (GDPR) and other relevant data protection frameworks. The following deficiencies and areas of concern were identified:

a. Privacy Policy – Material Gaps and Deficiencies

While DTEC provides a Privacy Policy, it does not currently meet several mandatory GDPR requirements:

•Lack of Specificity: The policy contains general descriptions of data processing but fails to clearly specify the purposes of processing, categories of data collected, lawful bases relied upon (e.g., consent, legitimate interests), data retention periods, or data recipient categories (Art. 13(1)(c–f)).

•Insufficient Detail on Blockchain Impact: Although blockchain is mentioned, the policy does not provide sufficient explanation regarding:

•the legal consequences of storing personal data (e.g., wallet addresses or vehicle identifiers) on an immutable ledger,

•the implications for users' ability to exercise rights such as rectification or erasure,

•and whether any pseudonymization or data minimization measures are in place to mitigate risks (Art. 5, Art. 25).

•International Transfers Not Covered: If any cross-border transfers occur (e.g., hosting or analytics services outside the EEA), the policy fails to provide the necessary safeguards or mechanisms in accordance with Chapter V of the GDPR.

b. Missing Cookie Policy

DTEC's website uses cookies and trackers (as observed during testing), yet no standalone Cookie Policy is available. A separate Cookie Policy is required under the ePrivacy Directive and GDPR to:

•Explain the types and purposes of cookies used (e.g., essential, analytics, marketing),

•Identify third-party providers involved,

•State retention durations,

•Inform users of their right to withdraw consent.

The absence of this policy represents a clear violation of the transparency and consent obligations set out in Art. 5(3) of the ePrivacy Directive and Art. 12–13 of the GDPR.

c. Non-Functional Cookie Consent Mechanism

During the assessment of the DTEC website, it was observed that no cookie banner or consent mechanism is present on the site, despite the use of cookies and tracking technologies (e.g., for analytics, performance, or user behavior monitoring). This represents a direct breach of the GDPR and the ePrivacy Directive.

In particular:

•Users are not provided with clear and prior notice regarding the types of cookies used or their purposes;

•There is no opportunity to provide or refuse consent before non-essential cookies are set;

•There is no option to manage cookie preferences, nor a mechanism to withdraw consent later;

•The Cookie Policy is entirely absent, which fails the transparency requirement under Article 12–13 GDPR and Article 5(3) of the ePrivacy Directive.

This omission constitutes a high-risk compliance gap, as supervisory authorities across the EU (including the Dutch DPA) have taken strict enforcement action against websites that deploy tracking technologies without valid consent mechanisms.

The lack of a cookie banner or consent layer also creates potential exposure to user complaints, enforcement actions, and administrative fines under Article 83 GDPR, especially if third-party services like Google Analytics or Meta Pixel are used without proper disclosures and opt-in controls.

d. Absence of Consent for Blockchain-Linked Personal Data

DTEC collects data that may constitute personal data under GDPR, such as:

•Wallet addresses,

•Vehicle identification data,

•Behavioral metrics linked to specific users.

This data is processed through a blockchain infrastructure, and yet:

•No explicit consent is obtained prior to the collection and recording of such data on an immutable ledger,

•Users are not adequately informed of the permanence or potential public accessibility of blockchain-stored information,

•There is no evidence of granular consent collection tied to specific data-sharing events or use cases.

This represents a high-risk compliance gap under Art. 6(1)(a) GDPR (lawfulness of processing) and Art. 7 (conditions for consent), particularly because blockchain processing may limit users' ability to later exercise their right to erasure (Art. 17).

e. Children's Data & Age Verification

Under Article 8 of the General Data Protection Regulation (GDPR), where the lawful basis for processing is consent, processing of personal data in relation to the offering of information society services directly to a child is only lawful if the child is at least 16 years old (or a lower age as permitted by Member State law, but not below 13). In the Netherlands, the applicable age of digital consent is 16.

If DTEC's Platform allows registration or data input by individuals under the age of 16—whether through direct sign-up, parental access, or passive data collection from connected vehicles—then appropriate age verification mechanisms must be implemented to ensure legal compliance. These mechanisms may include:

•A self-declaration age verification step during registration,

•Technical safeguards preventing minors from accessing core services,

•Parental consent workflows where applicable.

Even if DTEC does not intend to target or provide services to children under 16, the Privacy Policy must explicitly state that the Platform is not intended for individuals under 16 years of age, and that the Company does not knowingly collect personal data from children.

Failure to implement age verification procedures or to address children's data risks in the Privacy Policy may result in non-compliance with Article 8 GDPR, especially if behavioral or identifiable data of minors is collected without proper safeguards.

Given the nature of DTEC's services—particularly the integration with vehicles and use of reward-based systems—it is critical to ensure that consent is only obtained from individuals legally capable of providing it. Otherwise, any consent obtained from underage users may be deemed invalid, which could jeopardize the lawfulness of associated data processing operations.

4. Consent Management System – Design & Implementation Guidelines

To ensure lawful processing of personal data and transparency towards users in accordance with Articles 6, 7, and 13 of the GDPR and Article 5(3) of the ePrivacy Directive, DTEC must establish a robust, transparent, and user-controllable **Consent Management System (CMS)**.

Below are the key principles and technical steps for implementing a fully compliant CMS tailored to DTEC's platform architecture (including blockchain and in-vehicle data environments):

a. Consent Collection Principles (GDPR Art. 4(11), Art. 7)

Any consent collected from users must meet the following legal standards:

- **Freely given:** Users must not be forced or nudged into consenting by making it a condition to access core services.
- **Informed:** The user must be clearly informed of:

  - What data will be collected,
  - For what purposes,
  - By whom it will be used or shared,
  - Whether the data will be stored immutably on blockchain.
- **Specific:** Each purpose (e.g., analytics, marketing, data sharing with third parties, blockchain registration) must be presented as a separate, togglable option.
- **Unambiguous:** The user must give a clear affirmative action (e.g., ticking a checkbox or clicking "Accept") — **pre-ticked boxes are invalid**.
- **Documented:** DTEC must maintain **verifiable records** of when, how, and for what the user gave consent.
- **Withdrawable:** Users must be able to withdraw their consent **at any time**, as easily as they gave it.

b. 2. Implementation Steps for a Compliant Consent Layer

Step	Description
A. Deploy a Consent Banner or Pop-up	Upon the user's first visit, present a banner with concise info and access to full preference settings. Block all non-essential cookies and trackers by default.
B. Build a Preference Center	Allow users to manage and customize their consent preferences across categories (e.g., Necessary, Analytics, Marketing, Blockchain Data Logging). This should be accessible via footer link ("Privacy Settings").
C. Store Consent Logs Securely	Implement back-end infrastructure to log and timestamp user consent (what was consented to, when, and via what IP/device). These logs must be retrievable in the event of regulatory inquiry.
D. Enable Consent Withdrawal	Users must be able to withdraw their consent at any time with **no negative consequence**. This applies to cookie settings, marketing emails, and data submission to blockchain (where technically possible).
E. API-Level Integration (if relevant)	If DTEC offers developer-facing APIs, consent signals (such as TCF strings or hashed records) should be passed along to third parties to enforce lawful downstream processing.
F. Consent for Blockchain-Specific Use	Before any user data is linked to a blockchain transaction (e.g., wallet address, telemetry ID), present a **specific, additional consent screen**. Include an explanation that blockchain transactions are permanent and cannot be altered once published.

c. 3. Consent Management Tooling Options

DTEC can choose from the following implementation approaches:

- **Custom-built CMS:** Built in-house to match DTEC's unique ecosystem (e.g., handling blockchain data separately).
- **Third-party CMP (Consent Management Platform):** Use a GDPR-compliant CMP vendor such as:
  - **Cookiebot**, **OneTrust**, **Usercentrics**, or **TrustArc** — all of which offer customizable consent layers, preference centers, and automated compliance logs.
- **Hybrid model:** Implement core consent features in-house while integrating external CMP for cookie compliance.

d. 4. UX/UI Considerations for Compliance and Usability

- Use plain, user-friendly language (no legalese) in banners and preference centers.

- All consent options—“Accept All,” “Reject All,” and “Manage Preferences”—must be presented with equal prominence, using identical font size, color, and button dimensions to ensure a freely given and valid choice under GDPR.
- Provide visual indicators of consent status (e.g., toggles) and make it easy to revisit settings.

5. RISK AREAS AND RECOMMENDATIONS

This section outlines the key risk areas identified in DTEC’s data protection compliance posture, along with targeted recommendations for remediation in alignment with the GDPR and applicable EU data protection standards.

a. Absence of a Cookie Consent Mechanism

Risk Level: **High**

Description: No cookie banner or consent tool is implemented on the website, despite the use of cookies and potential third-party trackers. This results in a clear violation of Article 5(3) of the ePrivacy Directive and GDPR Article 7.

Recommendations:

•Implement a GDPR-compliant cookie consent solution with:

•Prior blocking of non-essential cookies,

•Granular choices (e.g., necessary, analytics, marketing),

•Easy withdrawal or update of consent.

•Create a standalone, user-friendly Cookie Policy detailing types of cookies, their purposes, retention periods, and third-party involvement.

b. Incomplete Privacy Policy

Risk Level: **High**

Description: Although some key elements (e.g., blockchain reference and data subject rights) are included, the Privacy Policy lacks sufficient detail on:

•Lawful bases for processing,

•Data retention periods,

•Categories of recipients,

•International transfers.

Recommendations:

•Update the Privacy Policy to include:

•A processing purpose and lawful basis matrix,

•Specific retention periods per data category,

•List or categories of third-party data recipients,

•Information on cross-border data transfers and applicable safeguards.

•Provide actionable instructions for users on how to exercise their rights, and disclose the contact details of the Data Protection Officer (if appointed).

c. No Age Verification or Statement on Children’s Data

Risk Level: **Medium–High**

Description: There is no age verification mechanism or explicit statement regarding whether the platform is intended for users under the age of 16, as required by Article 8 GDPR.

Recommendations:

•Add a clear statement in the Privacy Policy that the platform is not intended for users under 16.

•Implement a self-declaration mechanism during registration to confirm age eligibility.

•If services are targeted to minors in the future, introduce a verified parental consent mechanism.

d. Lack of Explicit Consent for Blockchain-Linked Data

Risk Level: Critical

Description: Personal data (e.g., wallet addresses, vehicle IDs) is recorded on blockchain without collecting explicit, informed consent from users. The immutable nature of blockchain poses a challenge to GDPR principles such as data minimization and the right to erasure.

Recommendations:

•Introduce a separate, informed, and specific consent flow before recording identifiable information on blockchain.

•Include disclaimers explaining:

•The irreversibility of blockchain records,

•The impact on data subject rights (e.g., erasure, rectification),

•Whether pseudonymization measures are used.

•Consider adopting a two-layer architecture (off-chain storage for identifiable data + on-chain pseudonyms or references).

e. No DPIA Conducted for High-Risk Processing

Risk Level: High

Description: Blockchain-based processing of personal data, particularly when linked to vehicles or behavioral profiling, qualifies as high-risk and requires a Data Protection Impact Assessment (DPIA) under Article 35 GDPR.

Recommendations:

•Conduct and document a DPIA that evaluates:

•The necessity and proportionality of blockchain processing,

•Specific risks to user rights and freedoms,

•Technical and organizational measures to mitigate such risks.

•Maintain the DPIA as a living document and update it with each substantial platform change.

6. Conclusion

This memorandum has examined the DTEC platform and its website from a GDPR compliance perspective. While the platform shows an initial awareness of data protection obligations—particularly through its integration of user rights and blockchain disclosures—there remain critical gaps that must be addressed to ensure full legal compliance.

Key deficiencies include the lack of a consent management mechanism, insufficient specificity in the Privacy Policy, absence of a cookie policy and age verification, and missing safeguards for blockchain-related data processing.

To meet GDPR standards and align with regulatory expectations, DTEC should prioritize implementing a Consent Management System, revising its legal documentation, and enhancing transparency and user control mechanisms across the platform.

Addressing these areas proactively will reduce legal risk, strengthen user trust, and support DTEC's long-term operational and regulatory sustainability.