CHEETAH DIGITAL

EU General Data Protection Regulation (GDPR) on Cheetah Loyalty

Features and Best Practices

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy.

Version	Date	Description	Reviewed / Approved by
1.0	August 2019	Initial release	Cheetah Digital Product Management
1.1	September 2021	Added version history	Cheetah Digital Product Management

Cheetah Digital, Inc., 72 W Adams St 8th floor, Chicago, IL 60603
Copyright © 2021 Cheetah Digital, Inc.
All rights reserved.
Printed in the United States of America

No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photographic, magnetic, or other record, without the prior agreement and written permission of Cheetah Digital.

Cheetah Loyalty, the Cheetah logo, and other Cheetah names referenced herein are trademarks of Cheetah Digital, and may be registered in certain jurisdictions.

Other product names, designations, logos, and symbols may be trademarks or registered trademarks of their respective owners.

PRODUCT MODULES AND OPTIONS. This guide contains descriptions of modules that are optional and for which you may not have purchased a license. As a result, your software implementation may differ from descriptions in this guide. To find out more about the modules your organization has purchased, see your corporate purchasing agent or your Cheetah Digital sales representative.
U.S. GOVERNMENT RESTRICTED RIGHTS. Programs, Ancillary Programs and Documentation, delivered subject to the Department of Defense Federal Acquisition Regulation Supplement, are "commercial computer software" as set forth in DFARS 227.7202, Commercial Computer Software and Commercial Computer Software Documentation, and as such, any use, duplication and disclosure of the Programs, Ancillary Programs and Documentation shall be subject to the restrictions contained in the applicable Cheetah Loyalty license agreement. All other use, duplication and disclosure of the Programs, Ancillary Programs and Documentation by the U.S. Government shall be subject to the applicable Cheetah Loyalty license agreement and the restrictions contained in subsection (c) of FAR 52.227-19, Commercial Computer Software - Restricted Rights (June 1987), or FAR 52.227-14, Rights in Data—General, including Alternate III (June 1987), as applicable. Contractor/licensor is Cheetah Digital, 72 W Adams St 8th floor, Chicago, IL 60603.

PROPRIETARY INFORMATION NOTICE

Stellar Loyalty, Inc. considers information included in this documentation and all Stellar Loyalty documents to be Confidential Information. Your access to and use of this Confidential Information are subject to the terms and conditions of: (1) the applicable Stellar Loyalty software license agreement, which has been executed and with which you agree to comply; and (2) the proprietary and restricted rights notices included in this documentation.

Contents

Introduction **4**

Scope and Timeline of the EU GDPR **5**
- What is the GDPR? 5
- Who Does the GDPR Apply To? 5
- What Happens to the Current EU Data Protection Laws after GDPR Comes Into Effect? 5

Main Principles of the EU GDPR **6**
- Increased Territorial Reach 6
- Data Subject Rights 6
- Data Privacy by Design and By Default 7
- Mandatory Breach Notification 7
- Data Protection Impact Assessment (DPIA) 7
- Data Protection Officers 7
- Significant Penalties for Non-Compliance 8

Cheetah Loyalty Compliance for the EU GDPR **9**
- AWS Compliance for the EU GDPR 9
  - AWS Features 10
  - AWS Compliance with CISPE Code of Conduct 10
  - AWS Data Breach Notifications 10
- Cheetah Loyalty Hosting Compliance for the EU GDPR 11
  - Data Encryption 11
  - Operational Reviews and Audits 11
  - Third Party Vulnerability Assessments 11
  - Cheetah Loyalty Breach Notifications 11
- Cheetah Loyalty Cloud Platform Features for the EU GDPR 12
  - Member Profile 12
  - Message Preferences 12
  - Message Templates 13
  - Member CSR Screen 13
  - Segments 13
  - Analytics and Dashboards 14
  - Roles and Permissions 14
  - Audit Trail 15

Best Practices for Brands to Comply with the EU GDPR **16**
- Create Awareness and Declare the Lawful Basis for Processing 17

Review and Update Privacy Policies 17
Collect Consent at Sign Up 18
Review Marketing Emails and Messages 18
Process Data Subject Requests At Least Monthly 19
Appoint a Data Protection Officer (DPO) 19
Prevent and Monitor for Security Breaches 19

Conclusion **20**

Introduction

At Cheetah Digital, we deliver the most powerful, flexible, and secure consumer loyalty and engagement solutions on the planet. Conforming with European Union data security and privacy regulations is a top priority for Cheetah Digital. This white paper describes Cheetah Loyalty's support for the EU General Data Protection Regulation (GDPR) that became enforceable on May 25, 2018.

As a cloud service provider, Cheetah Digital confirms that the Cheetah Loyalty Cloud Platform, in its role as the data processor, complies with the GDPR when it became enforceable on May 25, 2018. In addition, Cheetah Digital has entered into a data processing addendum (DPA) with Amazon Web Services to satisfy GDPR requirements for personal data that may be processed outside the EU.

As a Cheetah Loyalty customer, the brand is responsible for the environment once the service has been provisioned. Brands, in their roles as data controllers, must also review their compliance with EU GDPR and institute features and procedures to comply with EU GDPR. For example, brands should ensure that all consumer-facing screens request consent, ensure that every email has links for consumers to easily withdraw consent, configure access controls in the Cheetah Loyalty Marketing Console, and appoint a Data Privacy Officer.

Cheetah Digital, with the assistance of EU partners, has teams of compliance, data protection, and security experts who may assist brands in preparing and complying with EU GDPR requirements. For example, brands may want to enlist Cheetah Digital and/or an EU partner to act as a joint-controller by providing paid services, such as satisfying data subject rights, providing a Data Privacy Officer, or breach notifications. Please contact your Cheetah Digital account manager for more information about these EU GDPR services.

Scope and Timeline of the EU GDPR[1]

This section summarizes the scope and timeline the EU GDPR.

What is the GDPR?

In 2016, the European Commission approved and adopted the new General Data Protection Regulation (GDPR). The GDPR is the biggest change in data protection laws in Europe since the introduction of the EU Data Protection Directive, also known as Directive 95/46/EC, in 1995. The GDPR aims to strengthen the security and protection of personal data in the EU and harmonize EU data protection law. The GDPR will replace the EU Data Protection Directive, as well as all local laws relating to it.

The GDPR protects European citizens' fundamental right to privacy and the protection of personal data. It introduces robust requirements that will raise the bar for data protection, security, and compliance and will push the industry to implement stringent controls. GDPR creates consistency across EU member states on how personal data can be processed, used, and exchanged securely. Organizations will need to demonstrate the security of the data they are processing and their compliance with GDPR on a continual basis, by implementing and regularly reviewing robust technical and organizational measures, as well as compliance policies.

Who Does the GDPR Apply To?

The GDPR applies to all organizations established in the EU and to organizations, whether or not established in the EU, that process the personal data of EU data subjects in connection with either the offering of goods or services to data subjects in the EU or the monitoring of behavior that takes place within the EU. Personal data is any information relating to an identified or identifiable natural person.

What Happens to the Current EU Data Protection Laws after GDPR Comes Into Effect?

The GDPR will replace the existing Data Protection Directive (Europe Directive 95/46/EC). Beginning on May 25, 2018, the existing Data Protection Directive, and the laws relating to it, will no longer apply.

[1] Source: Amazon EU Data Protection website https://aws.amazon.com/compliance/eu-data-protection

Main Principles of the EU GDPR

The EU GDPR consists of over ninety articles with the goal to protect EU citizens from privacy and data breaches in a world that is significantly more data-driven from the establishment of the previous directive in 1995. Many of the 1995 data privacy key principles carry forward with the GDPR.

GDPR Article 5 enumerates the main principles. Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency")
2. Collected for specified, explicit and legitimate purposes
3. Limited to what is necessary in relation to the purposes ("data minimisation")
4. Accurate and kept up to date, and erased and rectified without delay ("accuracy")
5. Kept in a form that permits identification of data subjects for no longer than is necessary ("storage limitation")
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing ("integrity and confidentiality")

The rest of this section describes the key GDPR articles most pertinent to the use of Cheetah Loyalty Cloud Platform.

Increased Territorial Reach

GDPR Article 3 clarifies the territorial jurisdiction of the data privacy laws. The GDPR applies to all data controllers and processors that are established in the EU. However, GDPR also applies to the processing of personal data in the EU, regardless of whether the processing takes place in the EU or not.

Data Subject Rights

GDPR strengthens data protection for EU residents by requiring the right to access personal data, to correct inaccuracies in that data, to erase that data, to object to processing of their personal data, and to move that data. Key data subject rights include:

- Explicit Consent. GDPR Articles 7 and 8 strengthens the consent requirements by ensuring that consumers must opt-in and have access to intelligible and easy-to-access consent information. No more long illegible terms and conditions full of legalese. GDPR also includes specific regulations for parental consent for children under 16, and forbidding consent for children below 13 years of age.
- Right to Access. GDPR Article 15 advocates data transparency by specifying that data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

- Right to be Forgotten. GDPR Article 17 specifies that data subjects have the right to be forgotten when a consumer withdraws consent or the personal data is no longer relevant to the original purpose of processing. Consumers can request that data controllers erase personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.
- Right to Data Portability. GDPR Article 20 introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Data Privacy by Design and By Default

GDPR Article 25 calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. GDPR Article 23 specifies for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Mandatory Breach Notification

GDRR Articles 33 and 34 specify that data controllers must notify the supervising authority within 72 hours of becoming aware of a breach that may “result in a risk for the rights and freedoms of individuals”.

Data Protection Impact Assessment (DPIA)

GDPR Article 35 states that supervisory authorities may make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment. Hence, data controllers may need to conduct and to file a DPIA with the supervisory authority as needed. The DPIA will need to identify data handling procedures and processes, as well as the controls in place to protect personal data.

Data Protection Officers

GDPR Articles 37 to 39 describes the appointment of a Data Protection Officer who manages data security and other issues relating to the processing of personal data. DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. GDPR also streamlines processes by eliminating the need to submit registrations to each local DPA. Instead, the DPO must perform internal record keeping requirements.

Significant Penalties for Non-Compliance

GDPR Article 83 imposes substantial fines for data controller and processors that intentionally or inadvertently fail to comply with the GDPR.

Cheetah Loyalty Compliance for the EU GDPR

As a data processor, Cheetah Loyalty is supporting the rollout of the EU GDPR in four ways:

1. Verify AWS Compliance with GDPR. Cheetah Digital has reviewed and verified its underlying hosting infrastructure to ensure Cheetah Loyalty's compliance with EU GDPR. Cheetah Digital is hosting the Cheetah Loyalty Cloud Platform in the AWS EU Frankfurt region for brands that are based in the EU. For brands hosted in non-EU AWS regions (e.g. US-based brands), Cheetah Digital has executed a GDPR-approved Data Processing Addendum (DPA) with AWS.
2. Review Cheetah Loyalty Hosting Operations. Cheetah Digital has documented and audited its internal hosting processes and procedures, and successfully completed third-party vulnerability checks.
3. Implement GDPR-related Features The Cheetah Loyalty Cloud Platform provides numerous features to help brands comply with the GDPR data subject rights requirements, such as explicit consent, right to access, and the right to be forgotten.
4. Recommend Best Practices. Cheetah Digital has prepared a checklist of best practices for brands--as the data controller--to prepare and implement by May 2018. The checklist and best practices.

AWS Compliance for the EU GDPR

Cheetah Loyalty uses Amazon Web Services (AWS) as it's worldwide hosting provider. As such, Cheetah Digital has ensured that AWS complies with all GDPR requirements for a successful rollout in May 2018.

As of December 2017, AWS confirms that all AWS services will comply with the GDPR when it becomes enforceable in May of 2018.

> "AWS compliance, data protection, and security experts have been working with customers around the world to answer their questions and help them prepare for running workloads in the AWS Cloud after the GDPR becomes enforceable. These teams have also been reviewing everything that AWS already does to ensure it complies with the requirements of the new GDPR."[2]

In addition, Cheetah Digital, who has previously signed AWS's EU Directive Data Processing Agreement (EU Directive DPA), has also signed the new AWS Data Processing Agreement (GDPR DPA) that will meet the territorial requirements for the GDPR.

[2] Source: AWS EU Data Protection https://aws.amazon.com/compliance/eu-data-protection

©2019 Cheetah Digital. All rights reserved.

AWS Features

Cheetah Loyalty leverages numerous AWS features to meet the requirements of GDPR (see Figure 1). Brands can choose to host their Cheetah Loyalty Cloud Platform in the AWS EU Frankfurt region to ensure that personal data stays within the EU region.

Access Control: Control access to AWS resources

1. Allow only authorized administrators, users and applications access to AWS resources
2. Multi-Factor-Authentication (MFA)
3. Fine granular access to objects in Amazon S3-Buckets/ Amazon SQS/ Amazon SNS and others API-Request Authentication
4. Geo-Restrictions
5. Temporary access tokens through AWS Security Token Service

Monitoring and Logging: Get an overview about activities on your AWS resources

- Asset Management and Configuration with AWS Config
- Compliance Auditing and security analytics with AWS CloudTrail
- Identification of configuration challenges through AWS Trusted Advisor
- Fine granular logging of access to Amazon S3 objects
- Detailed information about flows in the network through Amazon VPC-FlowLogs
- Rule-based configuration checks and actions with AWS Config Rules
- Filtering and monitoring of HTTP access to applications with WAF functions in AWS CloudFront

Encryption: Encrypt Data on AWS

- Encryption of your data at rest with AES256 (EBS/S3/Glacier/RDS) Centralized managed Key Management (by AWS Region)
- IPsec tunnels into AWS with the VPN-Gateways
- Dedicated HSM modules in the cloud with AWS CloudHSM

Strong Compliance Framework and Security Standards:

- ISO 27001/9001 certified
- ISO 27017/27018 certified
- SOC 1 / SOC 2 / SOC 3
- Cloud Computing Compliance Controls Catalog (C5 - German Government-backed attestation scheme)

Figure 1: AWS Security Features[3]

AWS Compliance with CISPE Code of Conduct

AWS announced compliance with the CISPE Code of Conduct, which helps cloud customers assess how their cloud infrastructure provider complies with its data protection obligations under the GDPR. AWS has declared that the AWS services used by Cheetah Loyalty, including AWS EC2, AWS S3, AWS RDS, AWS IAM, AWS EBS, are fully compliant with the CISPE Code. More detail on AWS' compliance with the CISPE Code of Conduct can be found at https://cispe.cloud

AWS Data Breach Notifications

AWS has committed to notify its customers, including Cheetah Digital, without undue delay if AWS becomes aware of a breach of our security standards relating to the AWS network.

[3] Source: AWS EU Data Protection https://aws.amazon.com/compliance/eu-data-protection

©2019 Cheetah Digital. All rights reserved.

Cheetah Loyalty Hosting Compliance for the EU GDPR

Throughout 2017, Cheetah Digital's operations team has been working diligently to implement policies and procedures to prepare for the EU GDPR.

Data Encryption

The GDPR recommends pseudonymisation, a process that transforms personal data to a form that cannot be attributed to a specific data subject, to reduce the risks of a security breach. To this end, Cheetah Loyalty has implemented encryption to protect personal data from being read, copied, altered, or deleted by unauthorized parties without access to the correct decryption key. Cheetah Loyalty utilizes TLS v1.2 encryption for data-in-transit to the Cheetah Loyalty Cloud Platform. Cheetah Loyalty also provides the option to utilize AES-256 encryption for at-rest data to make the data illegible and unusable in case of a data breach.

Operational Reviews and Audits

Cheetah Digital conducts regular reviews and audits of its hosting infrastructure, including but not limited to frequent reviews of access and operational logs; proactive monitoring alerts; risk assessments; disaster drills; change management requests; and so on. These reviews are audited at least annually by a third-party assessment firm.

Third Party Vulnerability Assessments

Cheetah Digital enlists third party security firms to conduct vulnerability assessments to identify and classify potential security holes in the Cheetah Loyalty Cloud Platform. Cheetah Digital treats critical and high vulnerabilities with the utmost priority.

Cheetah Loyalty Breach Notifications

Cheetah Digital continually uses AWS-provided and third-party monitoring tools to identify, document and act-on privacy breaches against the Cheetah Loyalty Cloud Platform. Cheetah Digital shall notify brands without undue delay, if Cheetah Digital becomes aware of a breach that may "result in a risk for the rights and freedoms of individuals".

Confidential and Proprietary
©2019 Cheetah Digital. All rights reserved.

Cheetah Loyalty Cloud Platform Features for the EU GDPR

The Cheetah Loyalty Cloud Platform already includes a collection of administrative features to satisfy the GDPR's accountability principle. Controllers can use these administrative features to document decisions about processing activities and to comply with the GDPR's data subject rights requirements.

Member Profile

Cheetah Loyalty's Member Profile module provides the ability for Marketers to configure new member attributes and member preferences. Marketers can define member attributes to collect consent and other tracking data to comply with the GDPR. For example, Marketers can configure these three member attribute fields and populate these fields:

- Consent Processing: 'true' or 'false' based on consent given
- Consent Updated At: the date and time the GDPR Consent value was updated.
- Consent Notes: Any notes such as the purpose of processing and how the consent was obtained (e.g. web/mobile app checkbox, in-person, call center, etc.)

Then, expose these fields on the web, mobile, emails, and other channels so members can set these values. (FUTURE) The Cheetah Loyalty Cloud Platform logs changes to these member attribute fields to the member's activity history. Marketers can use the Member Activity History screen to document data subject's initial consent, changes to the consent, and removal of consent from the database. (FUTURE) In 2018, the Cheetah Loyalty Cloud Platform shall preconfigure the three consent fields to eliminate manual configuration in the future..

Message Preferences

Cheetah Loyalty includes pre-built email and push preferences for each member, such as opt-ins for receiving types of email and the frequency for receiving those emails. Marketers can view and edit these message preferences on web apps, mobile apps, and on the Member CSR screens. Cheetah Loyalty's Message module respects these pre-built message preferences when sending messages to recipients.

Figure 2: Example Message Preferences

©2019 Cheetah Digital. All rights reserved.

In addition, Marketers can create custom message preferences as needed. Marketers can also create new Cheetah Loyalty Segments to identify message recipients that match specific message preference values.

Message Templates

Cheetah Loyalty uses message templates, which are HTML files that define the layout and contents of each email and push message sent to members. Message templates can include links to a screen to let members change their message preferences, to unsubscribe from messages, or even to withdraw consent.

Member CSR Screen

Cheetah Loyalty includes a Member CSR screen, shown below, that provides a comprehensive view of a member's profile, preferences, and activity history. Data controllers can use this screen to satisfy GDPR Article 15 to "provide confirmation that an individual's data is being processed" and "to provide a copy of the personal data undergoing processing in a commonly used electronic form." Click on the 'Download All Activities' icon to export all of the member's activities into a readable csv file. Typically, data controllers must respond to individual requests within a month.

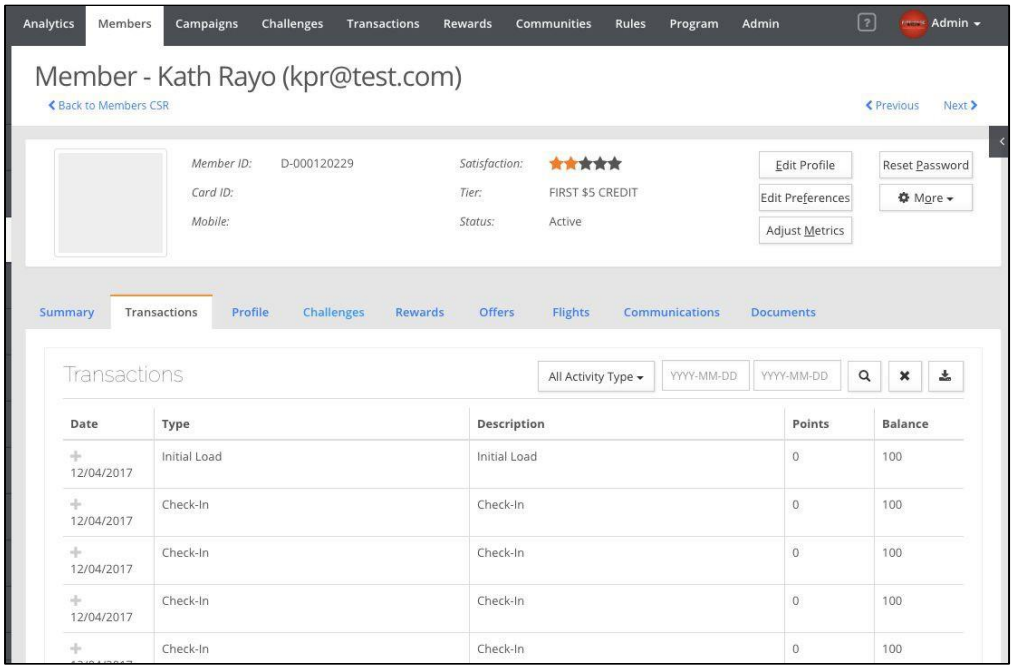


Figure 3: Cheetah Loyalty's Member CSR Screen

Segments

Cheetah Loyalty's Segments module lets marketers lists of members that match one or more conditions using member attributes, member preferences, and member activity histories. Marketers can export a segment's members to a csv file, or use these segments to target

©2019 Cheetah Digital. All rights reserved.

content and messages to sets of members. For example, just because a member is valid does not need mean that brands should send emails to them forever: brands can use segments to send marketing emails to members who have made a purchase in the last 180 days.

Analytics and Dashboards

Cheetah Loyalty's Analytics module lets marketers create queries and dashboards using any data stored in the Cheetah Loyalty Cloud Platform. For example, Marketers can create queries and dashboards showing data subjects who reside in the EU, have provided consent, or withdrew consent.

Roles and Permissions

Cheetah Loyalty includes several built-in roles for Marketing Console users:

- Admin: All parts of the Marketing Console, including the Admin screens
- CSR: Access to the
- Author: Access to content creation screens, such as Offers, Challenges, Rewards, Codes
- Analyst: Access to the analytics dashboards and queries

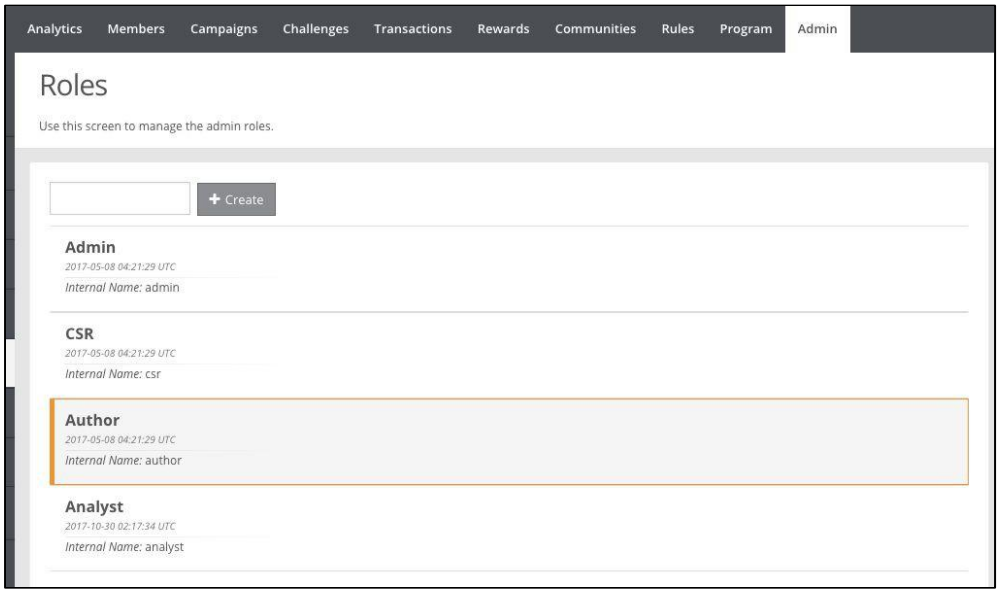


Figure 4: Cheetah Loyalty's Roles Screen

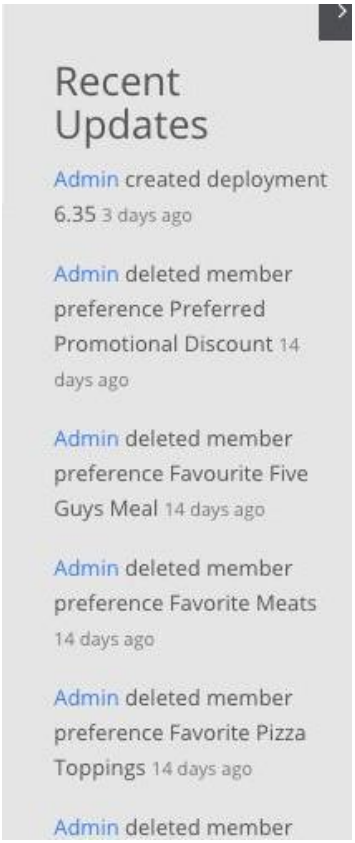
Brands can create custom roles to reflect the brand's own policies and role types. In general, brands should have a clear policy and defined process around the granting of roles. The best practice is to give the minimum role to each Marketing Console user and to conduct regular, at least quarterly, reviews of Marketing Console users.

©2019 Cheetah Digital. All rights reserved.

Audit Trail

Cheetah Loyalty includes an Audit Trail showing a history of changes to the Cheetah Loyalty Marketing Console, including:

- Changes to content items--such as challenges, offers, rewards, codes--and how last update it
- (FUTURE) Changes to member's attributes or preferences
- (FUTURE) History of successful and failed logins to the Cheetah Loyalty Marketing Console
- (FUTURE) History of successful and failed member logins to the Cheetah Loyalty Cloud Platform



Confidential and Proprietary
©2019 Cheetah Digital. All rights reserved.

Best Practices for Brands to Comply with the EU GDPR

As the data controller, each brand must proactively prepare and implement changes to comply for the EU GDPR. Use the checklist and best practices below to comply with the EU GDPR.

Below is a high level checklist from the UK's Information Commissioner's Office that brands, as data controllers, can use a guide for implementing the GDPR[4]:

Awareness. Make sure that decision makers and key people in your organisation aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

Lawful Basis for processing personal data. Document the personal data you hold, where it came from and who you share it with. You may need to organise an information audit. Identify and document the lawful basis for your processing activity in the GDPR, then update your privacy notice to explain it.

Communicating privacy information. Review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

Consent. Review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

Children. Put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

Data Subject's rights. Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

Subject access requests. Update your procedures and plan how you will handle requests within the new timescales.

Data Protection Officer. Appoint someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

Data Breaches. Make sure you have the right procedures in place to detect, report and investigate a personal data breach.

International. If your organisation operates in more than one EU member state, determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

[4] Source: https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

©2019 Cheetah Digital. All rights reserved.

Data Protection By Design and Data Protection Impact Assessments. Identify whether your supervising authority published the need to conduct impact assessments in your organisation.

Create Awareness and Declare the Lawful Basis for Processing

The first step is to ensure that the brand's senior management understand the rationale, key points, and the timeline for GDPR.

Cheetah Digital recommends that brands:

- Document the personal data stored in the Cheetah Loyalty Cloud Platform, including member attributes, member preferences, and member activity types the brand regularly collects for each member.
- Declare the lawful basis for processing personal data

For most brands conducting loyalty and engagement programs, Article 6, paragraph 1(a) is the most relevant lawful basis for processing:

> "the data subject has given consent to the processing of his or her personal data for one or more specific purposes"

Fortunately, most brands require members to sign up to join their loyalty and engagement programs.

Review and Update Privacy Policies

The next step is to review and update the brand's privacy policy to comply with GDPR requirements for consent-based processing of personal data.

Cheetah Digital recommends that brands:

- Review their privacy policy to include required GDPR information (see below)
- Make a link to the privacy policy clearly available on every sign up page

GDPR Article 13 states the privacy policy should include the following

- Identity and contact details of the Controller and the controller's representative to the EU
- Contact details of the Data Privacy Officer
- Purposes and legal basis of the processing of the personal data
- Recipients or categories of recipients with whom the data is shared
- Whether the controller intends to transfer personal data to a third country or international organization
- Period for which the personal data will be stored or the criteria used to determine the period,
- The right to request access to, rectification of, to erasure of, to objection to the processing of and to restriction of the processing of personal data

©2019 Cheetah Digital. All rights reserved.

- The right to withdraw consent at any time
- The right to lodge a complaint with a supervisory authority
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- Existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In addition, GDPR Article 7 states that "if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."

Collect Consent at Sign Up

Configure Cheetah Loyalty to get explicit consent from members in the sign up form. Note that the GDPR requires that consent be clearly communicated and that consent must be obtained on an opt-in basis. No functionality should be enabled by default, even if an opt-out function exists. Brands must make it easy for data subjects to changes their message and marketing preferences or to withdraw consent at any time.

Cheetah Digital recommends that brands:

- Configure the three consent member attributes, if they do not already exist
- Collect a consent checkbox on sign up page.
- Adopt a simple policy that prohibits usage by persons under 16 years old from signing up and clearly state this in the Terms of Service or Privacy Policy. If supporting under 16s is required, remember to implement an age check on the sign up page to ensure that members are at least 16 years old.
- Configure a Message Preferences page
- Provide an email or a page for member's to withdraw their consent

Review Marketing Emails and Messages

Consent to send messages is not necessarily forever. Instead of blasting messages to every single member records, brands should focus their marketing efforts on engaged members.[5] Focusing on engaged members also is an easy way to maintain a good reputation at major email providers.

Cheetah Digital recommends that brands:

[5] Source: GPRD: How New Email Laws Benefit Marketers https://sendgrid.com/blog/gdpr-how-new-email-laws-benefit-marketers/

©2019 Cheetah Digital. All rights reserved.

- Ensure that Message Templates include an unsubscribe link and/or links to the Message Preferences page
- Review marketing messages and use Cheetah Loyalty Segments to remove recipients who have stopped engaging with the brand, even without explicitly unsubscribing

Process Data Subject Requests At Least Monthly

Ensure that someone is responsible for monitoring and processing incoming data subject requests at least monthly.

Cheetah Digital recommends that brands:

- Use the Cheetah Loyalty Member CSR screen to export and send member activity history
- Deactivate members who withdraw their consent
- Use Segments to remove members from data processing
- Use Analytics and Dashboards to view trends and generate reports

Appoint a Data Protection Officer (DPO)

Cheetah Digital recommends that brands appoint a Data Protection Officer (DPO) to monitor compliance with the GDPR and other EU data protection provisions, to provide data privacy advice to the brand's employees, and to cooperate and act as a contact point for the supervisory authority.

The DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could results in a conflict of interest.

Prevent and Monitor for Security Breaches

Brands should use the Cheetah Loyalty Marketing Console to prevent and to proactively monitor for data breaches. Cheetah Digital commits to proactively notifying brands with undue delay after becoming of a data breach in the underlying hosting infrastructure.

Cheetah Digital recommends that brands:

- Review and assign Cheetah Loyalty Roles to Marketing Console Users at least quarterly
- Review the Cheetah Loyalty Audit Trail for breaches as often as possible

©2019 Cheetah Digital. All rights reserved.

Conclusion

At Cheetah Digital, we aim to deliver the most powerful, flexible, and secure consumer cloud platform in the world. Security is a top priority from day one and we continually monitor, test, and improve the Cheetah Loyalty Cloud Platform's security capabilities. Cheetah Digital has implemented numerous features and procedures to ensure that the Cheetah Loyalty Cloud Platform, and all underlying components such as AWS, are ready for the GDPR when it becomes enforceable in May 2018. Cheetah Digital continues to closely track applicable GDPR guidance issued by EU regulatory authorities.

Cheetah Digital strongly encourages the brands operating on the Cheetah Loyalty Cloud Platform to prepare for the GDPR now. For brands that have already implemented high levels of security and data privacy, the rollout of the GDPR is straightforward. For brands that have yet to start their GDPR projects, Cheetah Digital urges these brands to begin the review and implementation process as soon as possible, as described in this white paper:

- Understand the scope and impact of the GDPR
- Learn about the Cheetah Loyalty features for GDPR
- Use the Controller Checklist as a Guide to comply with the GDPR

Cheetah Digital, with the assistance of our EU partners, is always available to help brands make a smooth transition by May 2018.

Confidential and Proprietary
©2019 Cheetah Digital. All rights reserved.