Back4App
440 N Wolfe Road, Sunnyvale, CA, 94085

Information Security Manual

1. Revision Control

Version	date	author
V0.1	11-may-2018	Salvador Jorge da Cunha Ronconi - External Consultant - salvador@konatus.com.br

2. BACK4APP

Back4app is the world's most popular Parse Server as a service platform. We are a fully managed backend platform featuring automated provisioning and scaling of Parse Server applications, backup and recovery, 24/7 monitoring and alerting, web-based management tools, and expert support. This manual will detail how Back4App complies with GDPR requirements for Parse apps.

3. EXECUTIVE SUMMARY

In order to comply with EU GDPR Back4App developed a security program based on five elements:

- Use of GDPR compliant infrastructure
- Internal Policies;
- Record of processing activities;
- Regular review of protection measures;
- Adherence to established code of conduct.
-

The execution and maintenance of this security program will involve Back4App personnel. A key role on this program will be performed by an assigned Data Protection Officer(DPO). Safeguards as encryption, monitoring, logging and data privacy features are implemented using industry standard technologies. Most of the safeguards uses functionalities available from AWS - Amazon Web Services that are configured by Back4App to provide protections necessary to comply with GDPR.

In addition to technical measures Back4App established internal policies for confidentiality, access control, incident response and data retention. These policies are communicated to all employees and will be revised periodically. A risk assessment is performed and revised periodically to identify and evaluate the threats to information security and implement mitigation measures when necessary. Back4App established a risk assessment methodology based in five steps that follow GDPR recitals guidelines.

Back4App may transfer personal data across international borders. Any cross-border transfer of data must be supported by an approved adequacy mechanism detailed on the DPA - Data Processing Addendum.

Nevertheless, an Incident Response Plan was established to notify customers as soon as possible if Back4App becomes aware of unauthorized access to any customer personal data that results in loss, disclosure or alteration of that data.

Back4App uses third-parties to process customer data will maintain an up-to-date list of sub-processors authorised to process customer data.

Finally, Back4App undertakes to provide assistance to customers with the ability to rectify, erase, restrict or retrieve subject data. The customer may use this ability in the fulfilment of its obligations to respond to requests for exercising data subject's rights.

Index

Revision Control 1

BACK4APP 2

Executive Summary 2

Information Security Program 5

Safeguards 7

Encryption: 7

Monitoring and Logging: 7

Data Privacy : 9

Access Control 9

Password Policy 9

Keys Management 10

Multi-Factor Authentication 10

User Access Management 10

User Responsibilities 11

Software Package Updates 11

Risk Assessment 13

Data backup and restoration 15

Transfer of personal data to third countries 16

Incident Response Plan 17

Sub-processors 18

Assistance to Data Controller 19

Data removal 19

Data access and portability 19

Data rectification 19

Restriction of and object to processing 19

Data Controlled by Back4App 20

References 21

4. Information Security Program

In order to comply with EU GDPR Back4App developed an information security program based on five elements:

- Use of GDPR compliant infrastructure
- Internal Policies;
- Record of all processing activities;
- Regular review of protection measures;

The security program must be followed by all Back4App personnel. Back4App established a set of technical, administrative and physical measures to protect processed data, assure rights of data subjects and record processing activities. The following are the established security measures:

- Use industry standard encryption algorithms and technologies employed to protect data;
- Use monitoring and logging technologies employed to keep traceability of data transfer and execution of data processing;
- Use data privacy technologies employed to assure that Back4App customers controls their customer content;
- Follow a data retention policy;
- Follow an access control policy with industry standard authentication technologies;
- Follow a confidentiality policy;
- Perform risk assessment;
- Maintain an incident response process;
- Get consent from controllers about utilization of sub-processors;
- Establish contractual obligations with sub-processors.

These protection measures will be reviewed to evaluate its effectiveness in meeting the GDPR regulation when security incidents occur or suspicions are raised. Internal policies regarding information security are communicated to all Back4App personnel by the release of this manual, specific procedures and work instructions.

As the infrastructure of Back4App is provided predominantly by AWS, the concept of this security program is based on the code of conduct adopted by AWS. The execution and maintenance of this security program will involve Back4App personnel. A key role on this program will be performed by an assigned Data Protection Officer(DPO). To assure an independent treatment concerning security issues Back4App DPO will not be part the boards of directors.

Role	Responsibilities
Data Protection Officer (DPO)	- Keep registry of data processing activities - Notify controller in case of data breaches - Revise internal process periodically
Managing Directors	- Approve Information Security Manual - Assure that resources are available to implement and maintain the security program
Employees	- Notify DPO in case of data breaches - Protect passwords and other authentication means

5. Safeguards

Safeguards as encryption, monitoring, logging and data privacy features are implemented using industry standard technologies. Most of the safeguards uses functionalities available from AWS that are configured by Back4App to provide protections necessary to comply with GDPR. The detailed configuration procedure of the safeguards is detailed at "GDPR Safeguards Configuration Procedure". The configurations defines by default the highest level of protection.

Encryption:

GDPR compliant applications will use a specific infrastructure hosted at an AWS datacenter where encryption is applied to:

- EFS volumes, using KMS;
- EBS volumes;
- Buckets S3 (server side), using SSE-S3;
-

In these cases AWS manages the encryption keys. Encryption is also applied to MongoDB and Configuration files, using at rest encryption system. In this case, the encryption keys are managed by DPO. All data traffic between servers and between clients are performed using HTTPS and SSL. HTTPS protocol is selected for all GDPR compliant customers when a Load Balancer is created.

Monitoring and Logging:

Operations and access are logged and monitored by functionalities implemented in Back4App dashboard and functionalities available in AWS infrastructure. Log of operations performed through dashboards are performed in two levels:

- Log of App management operations;
- Log of data access and modification in the Apps.
-

Management operations like App deletion, digital certificate modification, inclusion of collaborators, export of data and analytics queries are logged identifying the user that performed the request. Logs for analytics and collaborators registration are available to the customer in the dashboard, other logs are maintained internally by Back4App and may be requested by customers.

The operations performed directly into Apps data through dashboard are logged identifying the masterkey used to access and manipulate the data.

Monitoring and logging of Back4App infrastructure is performed using AWS functionalities Cloud Trail and ELB logging. API requests are logged by user using ELB logging. This logs contains:

- Timestamp;
- Endpoint
- Identification;
- Associated classes

The logs are stored in database for one day and transferred to log files. The log files are encrypted and stored in S3. These logs are made available to the customer when requested. Back4App management of AWS account is monitored by CloudTrail. The following operations will be logged:

- Access and operations at AWS Management Console;
- EC2 operations (create, activate, deactivate, delete)
- Bucket S3 operations
- Athena queries operations
- Lambda code operations
- CloudFormation operations
- Tag operations

All the logs will be evaluated on internal and/or external audits. Internal audits will be coordinated by DPO according to procedure detailed at “GDPR Safeguards Configuration Procedure”. External audits will be executed by specialized third parties audit organizations and will be performed by customer request.

In addition to API requests and operations log several monitors are implemented to detect unauthorized calls or suspected usage. The following events are monitored and alarms are activated upon detection:

- Use of insecure protocols for use with HTTPS traffic
- Use of insecure ciphers
- Use of insecure web origins
- Use of more than one access key by a single user
- Presence of Customer Master Key scheduled for deletion
- Unauthorized API calls
- Sign-in without MFA
- Usage of root account
- Changes in policies
- Changes in configuration
- Authentication failure in AWS management console
- Disable or schedule deletion of customer created keys

- Changes in Security group
- Changes to NACL, network gateways, route tables or VPC

Data Privacy :

In order to provide a high level of data privacy several measures were implemented to assure that only authorized Back4App personnel have access to data from customer of Back4App customers. These measures concerns the following aspects:

- Avoid the use of root account and root account access keys;
- Avoid creation of users with full administrative privileges;
- Ensure that access policies are attached only to roles;

In addition to technical measures Back4App established a Confidentiality Policy that must be followed by all Back4App personnel. This policy is communicated to all employees which must sign a Confidentiality Term.

Access Control

Access control rules and procedures are required to regulate who can access Back4App information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing information in any format, and on any device. The measures established to manage access are the following:

- Enforcement of a password policy;
- Management of password and keys;
- Use of Multi-Factor Authentication (MFA);
- Granting of access only to groups or roles;
- Management of access permissions
- Clear definition of responsibilities for access control

Password Policy

A poorly chosen or misused password is a security risk and may impact upon the confidentiality, integrity or availability of computers and servers. A password policy is followed by Back4App personnel and is enforced to GDPR compliant customers when creating a password. A password will not be created if it does not comply with the following rules:

- At least one upper case letter;
- At least one lower case letter
- A mix of alpha and numeric, with at least one character of each type

- Minimum of 14 characters.
- Is different from two previous passwords

In addition to the password policy Back4App personnel are encouraged to follow these guidelines:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any part of your username within the password.
- Do not use the same password for systems

Keys Management

Management of encryption keys will be performed by two means depending on the responsible to the encryption. Keys generated by AWS will be managed by the use of AWS KMS, that will be configured by Back4App according to the procedures described in "GDPR Safeguards Configuration Procedure". Keys generated on the encryption of MongoDB and Configuration Files will be managed by Back4App DPO. In both cases keys will be set to rotate in at least 90 days.

Multi-Factor Authentication

Access to GDPR compliant infrastructure is possible only with use of Multi-Factor Authentication. .All Back4App employee that have access to AWS management console have the MFA option enabled.

User Access Management

Each user will be part of a group or role defined by DPO. The groups or roles will have access permissions to console, database and machines according to the activities that must be performed. Permissions must be defined in order to grant minimal and necessary access to each Back4App employee.

Creation of new users and allocation of users to groups and roles must be defined by DPO or Managing Director. Any request for access must be submitted to the Managing Director or DPO for approval. When an employee leaves Back4App access to computer and network must be suspended and user accounts and keys in AWS management console must be deleted.

Each user must have a unique login that is not shared with or disclosed to any other user. Each login is associated with an unique password that is requested at each new login.

User access rights will be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks

To protect infrastructure from unauthorized access the following measures are implemented:

- Restriction to S3 bucket public read and write permissions, including its access control list (ACL);
- Restriction to global send or subscribe to SNS topics
- Restrictions to public access of EBS snapshots
- No security group allows unrestricted ingress access to port 22 (SSH)
- No security group allows unrestricted ingress access to port 3389 (RDP)
- Allow access to Security Groups only from specific IPs
- Restriction to publicly shared machine images (AMI)

User Responsibilities

Users are responsible to prevent their login and password being used to gain unauthorised access to Back4App systems by:

- Following the Password Policy Statements outlined above.
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Not sharing login and passwords with other users
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing DPO of any changes to their role and access requirements.

Software Package Updates

Software packages like operational system and development tools may present vulnerabilities that can be exploited. Regularly the software packages vendors releases updates to remove or mitigate known vulnerabilities. In order to maintain the software used in development and support activities protected from security threats Back4App incorporates updates in the software packages according to the following criteria:

- Critical and important updates must be incorporated within one month of the update release;
- Moderated updates must be incorporated within six month of the update release
- Low or not security related updates must be evaluated whether to apply the security update

The security criticality ranking is normally defined by each software vendor according to a specific ranking. The following table shows a security criticality ranking to be used as reference:

Rating	Definition
Critical	A vulnerability whose exploitation could allow code execution without user interaction. These scenarios include self-propagating malware (e.g. network worms), or unavoidable common use scenarios where code execution occurs ***without*** warnings or prompts. This could mean browsing to a web page or opening email.
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. These scenarios include common use scenarios where client is compromised ***with*** warnings or prompts regardless of the prompt's provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
Moderate	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations.
Low	Impact of the vulnerability is comprehensively mitigated by the characteristics of the affected component.

6. Risk Assessment

Risk assessment is performed to identify and evaluate the threats to information security and implement mitigation measures when necessary. The Risk Assessment form presented on annex 2 must be fulfilled during the assessment and the actions derived from this activity must be followed by DPO. The DPO has an obligation to advise in respect of Risk Assessment, but is not required to carry out this activity by himself or herself or be exclusively responsible for it.

Risk assessment tasks should be delegated across the organisation, as appropriate. The role of the DPO should be to define high-level guidelines or methodology and to ensure monitoring and evidencing of the assessment and their outcome, including mitigation action definition and residual risk identification. GDPR prescribes that the risk level is determined by considering the "likelihood" and "severity" of the harms to the individual. Back4App risk assessment methodology is based in five steps:

1) Identify the potential harms associated with processing activities performed by controllers using Back4App platform;
2) Evaluate the severity of harms if they occur;
3) Evaluate the likelihood of harms considering only the nature and frequency of threats;
4) Identify mitigation measures to reduce risks considered high;
5) Evaluate residual risks and needs to implement more mitigation measures

GDPR recital 75 presents a list of harms that must be considered in Risk Assessment. These harms must be classified as high according to severity:

1) Discrimination;
2) Identity theft or fraud;
3) Financial loss;
4) Damage to the reputation;
5) Loss of confidentiality of personal data protected by professional secrecy;
6) Unauthorised reversal of pseudonymisation;
7) Other significant economic or social disadvantage;
8) Deprivation of rights and freedoms or prevention from exercising control over personal data;

Considering the possible harms particular attention should be done to processing that uses data containing:

1) racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
2) personal aspects, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
3) personal data of vulnerable natural persons, in particular of children; or
4) a large amount of personal data and affects a large number of data subjects.

Harms will be classified according the severity in limited or significant, and according to likelihood in likely and unlikely. The following matrix is used to determine the level of risk:

Risk Matrix		Severity	
		Limited	Significant
Likelihood	Unlikely	Low	Moderate
	Likely	Moderate	High

The risks considered high absolutely must be avoided or reduced by implementing mitigation measures. The risks considered moderate will be evaluated according to the technical and commercial feasibility to implement mitigation measures. The risks considered low will not request the implementation of any mitigation measure.

A wide range of risk mitigation measures may be considered, the most important are implementation of security measures, data governance or oversight mechanisms. The appropriate mitigation measures depend on context and should be chosen taking into account the risks involved, the cost of implementing and the effectiveness of these measures, their impact on the purposes, interests or benefits that are being pursued.

7. Data backup and restoration

Back4App maintains a backup process to assure that any data loss or corruption will not cause permanent damage. The backup process has the objective to:

- Conduct backup of data from customer application and databases;
- Conduct backup of configuration files
- Conduct backup of logs
- Protect backups with cryptography
- Recover and reconstitute lost or corrupted data

Databases are configured to have incremental backup performed on a hourly basis. Application machines are stateless and a machine image is stored by Back4App. S3 buckets that contains customer data and logs are versioning-enabled and the versions older than 90 days are deleted.

Backup of configuration files are performed each hour and data is retained in the following period:

- each hour in the last 24 hours;
- one backup per day in the last 30 days;
- one backup per month in the last three months.

Data backup will be cryptographed and key will be managed by AWS. Backup procedure assures that all data requested to be removed from the database will fade away and permanently disappear within 90 days. Detailed instructions to perform data backup and restoration are described in “Backup Procedure” internal document.

8. Transfer of personal data to third countries

Back4App may transfer personal data across international borders. Any cross-border transfer of data must be supported by an approved adequacy mechanism detailed on the DPA - Data Processing Addendum.

Back4App will provide to the customer information about the region and country where its data is stored and processed by, including if performed by sub-processors. For security reasons, only a general location (such as a city) will be provided to allow the customer to identify which EU Member State has jurisdiction over the customer for processing performed by the customer using the service.

The Data Transfer Agreement will document customer's consent and authorisation to Back4App or sub-processors access and process data using services hosted in a third country. It will also describe additional safeguards to enforce data subject rights and make available effective legal remedies for data subjects.

9. Incident Response Plan

If Back4App becomes aware of unauthorized access to any customer personal data on its equipment or in its facilities and such unauthorized access results in loss, disclosure or alteration of that data, Back4App will notify the customer without undue delay as specified on "Cyber and Privacy Incident Response and Management Policy".

Any Back4App employee is responsible to notify Back4App DPO when suspect of a data breach. This notification will be done by fulfilling the data breach notification form available in annex 1.

DPO will revise the data breach notification form, evaluate the impacts on personal data and if applicable send this notification to affected controllers.

Back4App personnel will be kept updated about the procedures related to data breach response by DPO that will inform about any modification on "Cyber and Privacy Incident Response and Management Policy"..

10. Sub-processors

Back4App shall obtain the customer's consent before authorising a third party sub-processor to access and process customer data. The customer's consent will be provided by signing the DPA - Data Processing Addendum. If the customer objects to a sub-processor, the customer may immediately terminate the Service Agreement for convenience or, if agreed by the customer and Back4App, immediately terminate the service or that part of the service which is provided by Back4App using the relevant sub-processor.

Back4App shall maintain an up-to-date list of sub-processors authorised to process customer data. This list must be easily accessible to the customer at the time of acceptance of the DPA and during its term.

Prior to engaging any new Third Parties that may Process or access Customer Data, Back4App will notify Customer by updating its list of Third Parties found at https://www.back4app.com/product/parse-gdpr/thrid-parties at least fifteen (15) days before it authorizes and permits such Third Parties to Process or access Customer Data.

11. Assistance to Data Controller

Back4App will provide assistance to customers with the ability to rectify, erase, restrict or retrieve subject data. The customer may use this ability in the fulfilment of its obligations to respond to requests for exercising data subject's rights.

Data removal

Any data removal will be performed upon request of the controller. This request will be processed by Back4App personnel following the Work Instruction "Data Subject Rights Request Procedure for Back4App". The data removal process will assure that all data from a specific subject is removed from Back4App databases, including log and backups. When a GDPR compliant customer requests the termination of service all data, except logs, are removed from Back4App database.

Data access and portability

Requests of access and portability of personal data will be received from the controller only. If any request is received from data subject, official authorities or other parts this request will be forwarded to the related controller. To respond to these requests a file in csv format will be generated according to Work Instruction "Data Subject Rights Request Procedure for Back4App" with all data subjects information and will be sent to controller. It is controllers responsibility to separate and transmit this file to specific data subject or another company designated by data subject.

Data rectification

Any manipulation of data is responsibility of controllers, including rectification of data subject information. Back4App will provide the customer with the ability to rectify customer data. Customers may use this ability in the fulfilment of its obligations to respond to requests for exercising data subject's rights. If any request of rectification is received by Back4App it will be forwarded to the related controler.

Restriction of and object to processing

Any restriction of processing or object to processing must be determined by the controllers.

12. Data Controlled by Back4App

This manual addresses the measures implemented from Back4App as a processor. The most part of the threats and risks related to personal data security and subject rights that may have contribution from Back4App are related to the processing of data on behalf of controllers.

However, Back4App receives and manipulates data from its customer acting as a controller. Relative to protection against threats and risks the same security program will be applied to data controlled by Back4App assuring the same level of security established for processing activities. In addition Back4App has revised its Privacy Policy with customers to explicitly declare how personal data from customers are processed and assure that the data subjects rights and freedoms will be fully respected.

13. References

1 – GDPR Handbook for Small Business, Olivier Staquet

2 – AWS Data Processing Addendum

3 – AWS Security Whitepaper

4 – Data Protection Code of Conduct for Cloud Infrastructure Service Providers

5 – CIS Amazon Web Services Foundations

6 - Methodology for Privacy Risk Management, CNIL (Commision Nationale de l'Informatique et des Libertés)

7 - The Risk-Based Approach in the GDPR: Interpretation and Implications, Gabriel Maldoff, CIPP/US, IAPP Westin Fellow

8 - Back4App Data Processing Addendum

ANNEX 1 - DATA BREACH REPORT

1. POINTS OF CONTACT

name	organisation	contact details
[Name]	[Role] [Organisation]	[Direct phone] [Email]

2. SUMMARY

[Summary of the event and circumstances – When, what, who, summary of incident…]

3. PERSONAL DATA IMPACTED

type	sensitivity	scope	likely consequences
[Name]	[Low/High]	[All customers]	[Likely consequences]
[DoB]	[Low/High]	[Employees hired after 2016]	[Likely consequences]
[Bank account details]	[Low/High]	[All employees]	[Likely consequences]

4. MEASURES TAKEN OR PROPOSED

measures	Date

5. CONCLUSION

[Serious/minor breach, likelihood of happening again…]

ANNEX 2 – RISK ASSESSMENT

1. REVISION CONTROL

date	author
[Date]	[Name], [Role] ([Email])

2. EXECUTIVE SUMMARY

[Short description of the personal data category]
[Purposes of processing]
[Risks identified and mitigation]
[Residual risk]

3. PERSONAL DATA CATEGORY

[Identification of type of data and data subjects]

4. PURPOSE OF PROCESSING

[Description of each purpose, legal basis and categories of personal data]

5. IDENTIFICATION AND QUANTIFICATION OF POSSIBLE HARMS

Possible Harms	Severity	Likelihood	Absolute Risk
[Name]	[Limited/Significant]	[Likely/Unlikely]	[Low/Moderate/High]

6. MITIGATION OF RISKS

[Description of measures to address the absolute risks identified as high]

7. Assessment of Residual Risk

[Assessment: residual risk at acceptable levels Yes or No]
[Description of necessity and proportionality of the processing]
[Suggestions for other mitigation of risk]