JIA COMMUNICATIONS

DATA PROTECTION POLICY

OCTOBER 2021

PT Jaya Impian Abadi
Jl. Antene I No. 5B RT 10/RW 01 Kel. Gandaria Utara, Kec. Kby. Baru, Jakarta Selatan, DKI Jakarta 12140
Telepon: (021) 72780974/Email: info@jiadreams.com

Contents

I. Data Subject Rights

Every client, employee, vendor, and all stakeholder who provides their data to JIA Communications has the following rights referring to the General Data Protection Regulation (GDPR):

1. Right of Access

Data subjects have the right to access their data which has been provided to JIA Communications. Data subjects are also entitled to receive information about what we do with the data. The full information about JIA Communications Data Protection Policy can be accessed on www.jiadreams.com.

2. Right to Rectification

Data subjects have the right to correct inaccuracies or complete the data they provide to JIA Communications. However, in certain circumstances, we may have to apply certain conditions to be able to correct the data, for example, because the correction may incur costs.

3. Right to be Deleted/Forgotten

Data subjects have the right to ask JIA Communications to delete their data under the following conditions:

a) Their data is no longer required in connection with the fulfillment of the data collection/processing purposes, or the expiration of certain contracts;
b) The data subject withdraws consent for the data processing and JIA has no legitimate interest in continuing the processing;
c) The data subject objected to the processing of personal data by JIA Communications;
d) Data subjects must delete their data to comply with legal obligations;
e) JIA Communications conducts processing of personal data illegally, not following the agreed contract and/or applicable law.

4. Right to Restriction of Processing

Data subjects have the right to ask JIA Communications to restrict their data processing under the following conditions:

a) Data subjects objected or considered the processed data to be inaccurate;

b) Data processing violates the agreed employment contract and/or applicable law;

c) Data subjects requires the restriction of such data for the establishment, exercise, or defense of legal claims.

5. Right to Data Portability

Data subjects have the right to receive their data which has been provided to JIA Communications, in a structured, commonly used, and machine-readable format and have the right to transmit those data to other parties without hindrance, where the processing is based on consent or a contract and technically feasible.

6. Right to Object

a) Data subjects have the right to object to the processing of their data by JIA Communications at any time.

b) If the data subject has objected, JIA Communications will no longer process their data unless JIA Communications can demonstrate a valid reason for the processing, including for establishing, exercising, or defending a legal claim.

c) JIA Communications will inform if a person's data will be processed and used for direct marketing purposes. This information will be conveyed clearly, explicitly, and separately from other information.

d) Data subjects have the right to object to the processing of their data for direct marketing purposes. After the objection is stated, JIA Communications will no longer process his/her data.

7. Data Subject Rights Services

Questions or requests regarding the Data Subjects Rights can be submitted directly via telephone, SMS, WhatsApp, or email to the following contact:

Name	: Arief Yudo Wibowo
Position	: Director of Operations
Phone/SMS/WhatsApp	: +62-813-1407-5699
Email Address	: arief@jiadreams.com

This contact line is active during business hours (9 AM - 6 PM), 7 days a week, and will respond to any questions or requests related to Data Subject Rights in less than 24 hours.

II. Data Privacy Governance

1. Data Classification

Classification	Definition
Confidential	Data is classified as Confidential when it is **regulated by Data Processing Agreement (DPA)**, and/or when unauthorized disclosure, alteration, or destruction of that data could cause **severe to moderate damage** such as Risks to the Rights and Freedoms of Natural Persons, may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage. Examples of this data include, but are not limited to, printed and digital documents related to Personally Identifiable Information (PII), asset ownership, copyrights, intellectual rights, financial statements, business management and strategic plans, etc. Processing Terms: a) Confidential Data treated with **highest level of security measures** including: • Data is backed up for security purposes by reference to the Data Processing Agreement (if any) and/or with the written consent of the data subject. • Backup data is stored in a separate computing system from the devices that are used daily. • The data storage device and its files are password protected which are only shared with authorized parties.

Confidential	• Prevent the unauthorised reading, copying, modification or removal of data media (data media control); • Prevent the unauthorised input, unauthorised inspection, unauthorised modification, or unauthorised deletion of stored data (storage control); • Prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control); b) JIA Communications ensured that Confidential Data can only be accessed by Employee/Sub-Contractor in the context of performing their duties and able to meet the following requirements: • Competent and qualified to perform the specific tasks/the limited purpose of the data processing assigned to him/her; • Has been authorized by JIA Communications management and already signed the appropriate Non-Disclosure Agreement (NDA); • Has been fully instructed about the procedures and statutory regulations relevant to the performance of the obligations of Processor under DPA. c) Processing data only allowed in **full compliance with Data Processing Agreement (DPA)**, Data Protection Policy, and by authorization/permission/any additional instructions issued by Data Subjects. d) Data transfer to a third party acting as Sub-Contractor is only allowed in the following condition: • Transfer data only for limited and specified purposes; • Ascertain that the Sub-Contractor is bound by NDA and can provide adequate data protection policy; • JIA Communications take reasonable and appropriate steps to ensure that the Sub-Contractor processes the data

Confidential	effectively based on agreement; • The Sub-Contractor required to notify if they can no longer meet the obligation to provide adequate data protection; • JIA Communications take reasonable and appropriate steps to stop and remediate unauthorized/risked processing.
Private	Data is classified as Private when it is **not regulated by Data Processing Agreement (DPA)**, and unauthorized disclosure, alteration, or destruction of that data could cause **moderate to low damage**. Examples of this data include, but are not limited to, printed and digital documents related to event management plans and reports, production plans, event documentations, etc. Processing Terms: a) Private Data treated with **high level of security measures**, including: • Data is backed up for security purposes by reference to the Data Processing Agreement (if any) and/or with the written consent of the data subject. • Backup data is stored in a separate computing system from the devices that are used daily. • The data storage device and its files are password protected which are only shared with authorized parties. • Prevent the unauthorised reading, copying, modification or removal of data media (data media control); • Prevent the unauthorised input, unauthorised inspection, unauthorised modification, or unauthorised deletion of stored data (storage control);

Private	• Prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control); b) JIA Communications ensured that Private Data can only be accessed by Employee/Sub-Contractor in the context of performing their duties and able to meet the following requirements: • Competent and qualified to perform the specific tasks/the limited purpose of the data processing assigned to him/her; • Has been authorized by JIA Communications management and already signed the appropriate Non-Disclosure Agreement (NDA); • Has been fully instructed about the procedures and statutory regulations relevant to the performance of the obligations of Processor under Data Protection Policy. c) Processing data only allowed in full compliance with Data Protection Policy, and by authorization/permission/any additional instructions issued by Data Subjects. d) Data transfer to a third party acting as Sub-Contractor is only allowed in the following condition: • Transfer data only for limited and specified purposes; • Ascertain that the Sub-Contractor is bound by NDA and can provide adequate data protection policy; • JIA Communications take reasonable and appropriate steps to ensure that the Sub-Contractor processes the data effectively based on agreement; • The Sub-Contractor required to notify if they can no longer meet its obligation to provide adequate data protection; • JIA Communications take reasonable and appropriate steps to stop and remediate unauthorized/risked processing.

Public	Data is classified as Public when it is **not regulated by Data Processing Agreement (DPA)**, and unauthorized disclosure, alteration, or destruction of that data **could cause low to no damage.** Examples of this data include, but are not limited to, printed and digital documents related to company profile, company contact information, employee contact information, job advertisement, press release, etc. Processing Terms: a) Public data treated with **reasonable and appropriate level of security measures.** b) All persons are able to access Public Data.

2. Information Security Roles and Responsibilities

Classification	Data Type	Roles in Charge	Name
Confidential	Personally Identifiable Information (PII)	Director of Operations	Arief Yudo Wibowo
		Director of Productions	Jilmi Astina Anif
		Head of Administrator	Ahmad Sopian
	Client's Brief/Business/ Strategic Plans	Director of Operations	Arief Yudo Wibowo
		Director of Productions	Jilmi Astina Anif
	Legal/Business Contract	Director of Operations	Arief Yudo Wibowo
		Director of Productions	Jilmi Astina Anif
		Head of Administrator	Ahmad Sopian
		Director of Productions	Jilmi Astina Anif
	Financial & Tax Information	Director of Productions	Jilmi Astina Anif
		Head of Finance	Yanita Anif
		Head of Administrator	Ahmad Sopian
Private	Event Management Plans, Event Reports, Production Plans, Company Policy, etc.	Director of Productions	Jilmi Astina Anif
		Head of Productions	Aprizal Nur
		Head of Administrator	Ahmad Sopian
		Project Coordinator	Ismail Adi Nugroho
		Content Strategist	Adi Ahdiat
Public	Company Profile, Press Release, etc.	Director of Operations	Arief Yudo Wibowo
		Content Strategist	Adi Ahdiat

III. Data Retention

What We Collected	What We Do	Storage Period
Personally Identifiable Information (PII)	We collect this type of data to providing services to Data Subjects in full compliance with Data Processing Agreement (if any), our Data Protection Policy, and by authorization/permission from Data Subjects. Our services include making marketing tools, marketing programs, producing souvenirs/gimmicks, and organizing events according to the interests and needs of data subjects. We may use your data for maintaining business relationship and providing hospitality services, such as sending birthday wishes and gifts. We also may use your data for marketing communication needs, such as sending promotional items, sending sweepstakes prizes, or analyzing consumer data based on the Data Subjects' consent.	We will retain this data and delete it maximum 1 year after termination of the Data Processing Agreement (DPA); Or Immediately delete it if requested to do so by DPA Controller/Data Subject.
Client's Brief/Business/ Strategic Plans/ Legal/Business Contract	We collect this type of data to providing services to our Client in full compliance with Data Processing Agreement (if any), our Data Protection Policy, and by authorization/permission from Data Subjects. Our services include making marketing tools, marketing, programs, producing souvenirs/gimmicks, and organizing events according to the Client's interests and needs.	We will retain this data and delete it maximum 1 year after termination of the Data Processing Agreement (DPA)/Contract; Or Immediately delete it if requested by DPA Controller/Data Subject.

Event Documentation	We collect event documentation in the form of videos and photos which may contain Personally Identifiable Information (PII) but are not regulated in the Data Processing Agreement with certain clients, or we have not received permission from the Data Subject because the documentation is not intended to record/take pictures of certain people.. We use those videos and photos to create reports to clients, and to create our company profiles that may be publicly displayed on printed media, websites, social media, or another digital publication form. If there is a Data Subject who object or does not give consent to this action, please contact our Data Subject Rights Service to request deletion.	We will retain this data and delete it maximum 3 years after the event completion; Or Immediately delete it if requested by Data Subject.

IV. Data Protection Policy

1. Employees/Sub-Contractors are required to maintain the security of JIA Communications data and the parties it represents;
2. Employees/Sub-Contractors are prohibited from giving access and distributing JIA Communications data and the parties it represents in any form to other parties without written approval from JIA Communications management;
3. Employees/Sub-Contractors aren't allowed to make public statements through online media, social media, websites, chat forums, bulletin boards, blogs, etc, about the work being handled and all matters related to JIA Communications and the parties it represents, except for Employees/Sub-Contractors who are authorized with the written consent from JIA Communications management;
4. Employees/Sub-Contractors aren't allowed to write books, letters, articles, or other forms of writing containing information and facts related to JIA Communications and the parties it represents without the written consent from JIA Communications management;
5. Employees/Sub-Contractors aren't allowed to duplicating JIA Communications' data and the parties it represents without permission from JIA Communications management;
6. Employees/Sub-Contractors aren't allowed to falsify company documents, signatures, and other dishonest actions that cause material and immaterial damage to JIA Communications and the parties it represents;
7. If Employees/Sub-Contractors receive a fax/email/or any form of printed/digital document intended for the JIA Communications and the parties it represents, he/she must directly forward it to JIA Communications management;
8. Employees/Sub-Contractors are required to store company data neatly and safely in full compliance with JIA Communications Data Protection Policy to avoid a data breach;

9. JIA Communications will conduct investigations and file lawsuits against Employees/Sub-Contractors who are indicated to have caused a loss, misuse, unauthorized access, disclosure, alteration, and destruction of JIA Communications' data and the parties it represents;
10. Employees/Sub-Contractors who are convincingly proven to have caused a loss, misuse, unauthorized access, disclosure, alteration, and destruction of JIA Communications' data and the parties it represents are obliged to fully indemnify all losses, claims, damages, fees, and expenses incurred as a result of the breach;
11. JIA Communications will also impose sanctions on Employees/Sub-Contractors who are convincingly proven to be aware of cases of data breaches, but delay or intentionally fail to report them to management.

V. Background Check Procedure

To ensure the company's data security and prevent other criminal cases that may be committed by employees, JIA Communications conducts background checks on (1) prospective employee and (2) existing employees who will be promoted.

1. **Identity Verification:** Validates the applicant's ID Card number, date of birth, marital status, and current domicile address.

2. **Previous Employment Verification:** Confirming previous employment experience to the last two employers or employer in the last five years that the applicant claims, including:
   a) Date of employment;
   b) Job position;
   c) Quality of working performance;
   d) Reason for leaving work;
   e) Eligibility for re-employment;
   f) Other additional information related to the applicant.

3. **Personal and Professional References:** Contact at least two persons listed as references by the applicant, including:
   a) Family or relative;
   b) Superior or colleague in a professional work environment.

4. **Education Verification**: Validates the applicant's last claimed diploma/education status.

5. **Vehicle Number Verification**: Record the applicant's vehicle number.

6. **Credit History Verification:** Credit history check is only performed for positions that involve fund management.

7. **Criminal History Verification**: Applicants are required to submit a latest police certificate to prove whether they have a criminal history or not. If an applicant has a criminal history, the company will consider the following factors:
   a) The nature of the crime and its relationship to the job position;
   b) The number of criminal cases;
   c) Time since sentencing;
   d) The potential risks related to the job's position if the applicant hired;
   e) JIA Communications will always prioritize hiring or promoting applicants with no criminal history.

8. **Background Check Data Processing**: Background check data will be processed based on the consent of the applicant/employee for the purposes of the recruitment, the performance of the contract, and for the termination of the employment relationship.

VI. Training & Awareness

1. To ensure JIA Communications data security, Employees are required to attend basic data protection training once a year
2. Employees and Sub-Contractors also required to attend data protection briefing regularly before starting a project, and as soon as possible after a case occurs.
3. The training materials include:
   a) What are a data breach and examples of cases (online and offline);
   b) What are the risks of data breach for personal and company;
   c) What are the regulations and penalties for data breaches;
   d) What is Data Classification and how to apply it;
   e) What is Information Security Roles and Responsibilities and how to apply it;
   f) What is the procedure for processing data according to Data Processing Agreement (DPA) from certain clients;
   g) What to do when data breach occurs (online and offline);
   h) How to protect online data;
   f) How to activate the 2-step verification system on email and WhatsApp.
   g) How to check email security regularly once month using Avast Hack Check or other platforms available on the internet.
   h) How to protect offline data.
4. The training materials will continue to be developed and updated based on case findings and the latest trends.

VII. Record of Data Processing

To ensure JIA Communications data security, Employees who have received data processing authorization are required to fill out Data Processing form in performing their duties. For examples as follows:

No.	Date	Classification	Type of Data	File/Document	Processor/ Sub-Processor	Processing/Action
1.	17 Sep 2021	Confidential	Legal Contract	**PDF File (Original)** **Title:** Data Processing Agreement Between PT Shell Indonesia and PT Jaya Impian Abadi	☑ **NDA** Director of Operations - Arief Yudo Wibowo	Transferred the data to the Content Strategist - Adi Ahdiat by email to perform tasks: • Reviewing the provisions of the PT Shell Indonesia Data Processing Agreement (DPA) • Integrate these provisions into JIA Communications' Data Protection Policy
2.	22 Sep 2021	Private	Company Policy	**Microsoft Word File (Original)** **Title:** JIA Communications Data Protection Policy	☑ **NDA** Content Strategist - Adi Ahdiat	Transferred the data to the Director of Operations - Arief Yudo Wibowo by email to be reviewed.
3.	27 Sep 2021	Private	Company Policy	**Microsoft Word File (Revision 1)** **Title:** JIA Communications Data Protection Policy	☑ **NDA** Content Strategist - Adi Ahdiat	• Update writing structure • Fix writing errors/typos • Add company logo Transferred the data to the Director of Operations - Arief Yudo Wibowo by email to be reviewed.

VIII. Data Breach Incident Management

1. Preparation

a) JIA Communications develops Data Breach Incident Management to take reasonable and appropriate measures to protect data from loss, misuse, unauthorized access, disclosure, alteration, and destruction, taking into due account the risks involved in the processing and the nature of the personal data, and updates it regularly based on case findings.

b) The Director of Operations sets the Data Classification, the Information Security Roles and Responsibilities, and closely monitors its implementation.

c) The Director of Operations back up Confidential/Private data for security purposes by referring to the Data Processing Agreements (if any) and/or with written approval from the data subject. The backup data will be stored in a separate computing system from the devices that are used daily. The data storage device and its files also protected with a password which is only shared with authorized parties.

d) Every prospective employee is required to follow the Background Check Procedure before hired or promoted.

e) Employees are required to attend basic data protection training once a year.

f) Employees and Sub-Contractors are required to attend data protection briefing regularly before starting a project, and as soon as possible after a case occurs.

i) Employees are required to activate the 2-step verification system on email and WhatsApp.

j) Employees are required to check email security regularly once month using Avast Hack Check or other platforms available on the internet.

k) Employees and Sub-Contractors must sign a Non-Disclosure Agreement (NDA) before being accepted for work/before starting a project. The NDA contains the provisions described in the Data Protection Policy (section IV).

2. Identification

a) When a data breach occurs, or an indication/potential of a data breach are found, party related to the case must report immediately in less than 24 hours to his/her supervisor and the Director of Operations.

b) If the case is related to client's data, the Director of Operations must immediately forward the report to the client concerned in less than 24 hours. The report shall at least contain the following information:

- What case happened?
- When did it happen?
- Who found it?
- How was the case found?
- What actions will the company take?

c) **If the case relates to Shell's data, the report shall be submitted in less than 24 hours by email to cert@shell.com and cc the contract holder.** The report may also submit via **https://shell.alertline.eu/gcs/welcome.**

3. Containment

a) If an online data breach occurs, or an indication/potential of a online data breach are found, the Director of Operations immediately take the containment actions such as:

- Revoking any access rights on the internet account that the hacker is exploiting;
- Disseminate information and call for vigilance to those directly affected, or those who may be affected;
- Disconnect each device from the internet network by turning off Wi-Fi at the router and any access points;
- Unplugging any ethernet cables;
- Unplugging USB drives and other removable drives from the system;
- Trace the responsible party associated with the data, by checking records of data classification and data handling;

- Reporting cases of data breaches to the police and the Ministry of Communication and Information for further investigation.

b) If an offline data breach occurs, or an indication/potential of a offline data breach are found, the Director of Operations immediately take the containment actions such as:
   - Disseminate information and call for vigilance to those directly affected or those who may be affected;
   - Trace the responsible party associated with the data, by checking records of data classification and data handling;
   - Reporting suspected perpetrators of data breaches to the police for further investigation.

4. Eradication

a) In online data breaches case, JIA Communications will works closely with the police and the Ministry of Communication and Information to conduct investigations and take legal action against the perpetrators, and also cooperate with third-party IT technicians to eradicate hacker threats from the company's online system.

b) In offline data breaches cases, JIA Communications will cooperate with the police to conduct investigations and take legal action against the perpetrators, and fire employees who have been convincingly proven to have committed a data breach

5. Recovery and Lesson Learned

a) After an online data breach has occurred, and the source of the problem has been eradicated, JIA Communications reinforce online security system with the help of third-party IT technicians, and strengthens the Data Breach Incident Management based on the weaknesses found in the case.

b) After an offline data breach has occurred, and the source of the problem has been eradicated, JIA Communications reinforce the Information Security

Roles and Responsibilities, and strengthens the Data Breach Incident Management based on the weaknesses found in the case.

c) The Director of Operations evaluates and updates the Data Breach Incident Management by answering the following questions:
   - What weakness did the breach exploit?
   - What changes need to be made?
   - How should employee be trained?
   - How to ensure a similar breach doesn't happen again?

d) Director of Operations conducts training on updated Data Breach Incident Management to all employees.

e) Director of Operations socialize the updated Data Breach Incident Management to all Clients and other stakeholders.

IX. References

1. General Data Protection Regulation (GDPR)
2. Privacy Shield Principles
3. Guidelines for Data Classification - Information Security Office (ISO) Carnegie Mellon University
4. Cyber Incident Response Plan - Cyber Management Alliance
5. Data Processing Agreement (DPA) Between PT Shell Indonesia and PT Jaya Impian Abad, Effective Date 27th April 2016