External Parties Information Security Procedure

Version number: 1.0

Publish date: 16-05-2018

Document control	
Prepared by	Mike Moore, Managing Director
Authorised by	Upper Management
Physical Copy location(s)	Operations Folder
Source Copy Location(s)	Dropbox - GDPR123\Documents\Final Documents
Published Copy Location(s)	www.Dephoto.biz\GDPR
Other Referenced Documents	
Related Material	
Acknowledgements	GDPR123
Distribution	Upper Management, Franchise Owners, All Staff

Version Control				
Title	External Parties Information Security Procedure			
Description	External suppliers appointed to process data shall be compliant with all relevant legislation regarding data protection such as the GDPR.			
Created by	Mike Moore			
Date Created	16-05-2018			
Maintained by	Upper Management			
Version Number	Modified By	Modifications Made	Date Modified	Status
1.0	Mike Moore	First creation	16-05-2018	Published

Contents

Purpose

To control access to DE Photo (Franchising) Ltd (referred to as the company here after) information and information systems by third parties who are contracted to design, develop, operate information systems or process data on behalf of the company.

All external suppliers used shall agree to adhere to the IT Security Policies, Procedures, Related Guidance and supporting regulations. The policy, or the elements of the policy relating to access by third parties, shall be delivered to any supplier before the supply of any services or the processing of data.

External suppliers appointed to process data shall be compliant with all relevant legislation regarding data protection such as the GDPR.

Prerequisites

For this procedure to be followed the following conditions need to be met:

- All parties need to be aware of their roles and responsibilities.
- Any systems/services/devices referenced need to be available to the relevant parties.
- All parties have had the relevant training and the training is current and up to date.
- A document register or system to track and record all external parties' policies and procedures must be in place and be readily accessible.
- External parties shall have an appropriate security policy available for scrutiny.
- External parties shall have relevant information security procedures available for scrutiny.
- The supporting documents need to be current and available to the relevant parties.

Conditions

This procedure should be followed if the company enters into an agreement for an external company to undertake processing on their behalf.

Outcomes

External parties are shown to be compliant and have an adequate level of information security to process data.

Process

1. Access document register
2. Gather all relevant external parties' information security policies and procedures
3. Record the author of the external party's information security policies and procedures
4. Record the location of the external party's information security policies and procedures
5. Record the creation date for the external party's information security policies and procedures
6. Record the last review date for the external party's information security policies and procedures
7. Record when the next review date is for the external party's information security policies and procedures
8. Make sure there is an automated calendar to hold and maintain review dates of the external party's information security policies and procedures.
9. Make sure the external party's information security policy had a procedure for reviewing third parties' information security
10. Check to make sure external parties' information security policies and procedures are being adhered to
11. Check to make sure all external parties' information security procedures include steps to obtain a binding agreement that the third party shall adhere to {company name}'s security standards.
12. Provide all external parties with data controller contact information and if needed Data Protection Officer contact details
13. Have a team of staff members review all external parties and assess them for non-compliance
14. Make sure all external parties' policies include responsibilities and obligations of processing data
15. Check external parties' policies for PCI Scanning or similar regular vulnerability scanning processes on public facing systems and applications
16. Record in the document register whether the external party's information security policy conforms to your level of compliance

Management and Review

This policy should be reviewed as scheduled once annually unless performance indicators, changes to legislation or the organisation necessitate it.

Last Review Date: 16/05/2018

Next Review Date: 16/05/2019