GDPR Process for requests of data subjects

GENERAL PROCESS INFORMATIONS	
Process Name	GDPR requests of data subjects
Process Owner	Schaefer Alexander
Date Created	2018-05-05
Last Update by	
Last Update date	
Last revision Date	
Process Purpose	The purpose of this process is how to react on formal requests of data subjects regarding their stored personal data.

Process Flow:

1) only written requests can be accepted. Please ask for a written request.

2) every request has to be forwarded to the local Data Protection Coorinator (DPC) and to the Group CIO

3) The DPC will start the identifiaction process. The requester must be identified in such a way that we are sure that the request comes from the person for whom he or she claims to be.

A possible answer to the request could be:

We would be happy to provide you the requested information! Please send us a copy of your identity card via your email address in order to identify you as a user of our services. Please black out all information except picture, name and date of birth. Only after successful verification may we forward your data to you.

4) If the person is an employee or former employee the information goes to HR department and General Manager of the country.

5) The DPC will intruct the responsible persons of personal data processing (according to our record of privacy data processing) to collect the information about the requestor.

a) If the person is a customer or user of our services (eXite, eXite Pro, TradeIT, submIT, TrustIT, BuyIT, location finder or other connected services) we have to collect the stored data manually from the services used by the requestor. In addition, if this person has accounts at our suppliers/service providers (e.g. Panteon) we have to request the information from the effected service provider.

b) we have to manually collect all information stored in local CRM system about the requestor.

c) we have to manually collect all information stored in our Billing system about the requestor.

d) if the requestor is an employee or former employee we have to manually collect all information stored in HR systems.

e) The record of privacy data processing has to be checked if any other processing can be relevant for the requestor. And if yes, also this information has to be collected manually.

6) After collection, the information will be put together by the DPC and forward it to the requestor.

GDPR Process for requests for correction of data subjects

GENERAL PROCESS INFORMATIONS	
Process Name	GDPR deletion requests of data subjects
Process Owner	Schaefer Alexander
Date Created	2018-05-05
Last Update by	
Last Update date	
Last revision Date	
Process Purpose	The purpose of this process is how to react on formal correction request of a data subjects regarding their stored personal data.

Process Flow:

1) only written requests can be accepted. Please ask for a written request.

2) every request has to be forwarded to the local Data Protection Coorinator (DPC) and to the Group CIO

3) The DPC will start the identifiaction process. The requester must be identified in such a way that we are sure that the request comes from the person for whom he or she claims to be.

A possible answer to the request could be:

We would be happy to correct the requested information! Please send us a copy of your identity card via your email address in order to identify you as a user of our services. Please black out all information except picture, name and date of birth. Only after successful verification may we forward your data to you.

4) If the person is an employee or former employee the information goes to HR department and General Manager of the country.

5) The DPC will intruct the responsible persons of personal data processing (according to our record of privacy data processing) to collect the information about the requestor.

a) If the person is a customer or user of our services (eXite, eXite Pro, TradeIT, submIT, TrustIT, BuyIT, location finder or other connected services) we have to collect the stored data manually from the services used by the requestor. In addition, if this person has accounts at our suppliers/service providers (e.g. Panteon) we have to request the information from the effected service provider.

b) we have to manually collect all information stored in local CRM system about the requestor.

c) we have to manually collect all information stored in our Billing system about the requestor.

d) if the requestor is an employee or former employee we have to manually collect all information stored in HR systems.

e) The record of privacy data processing has to be checked if any other processing can be relevant for the requestor. And if yes, also this information has to be collected manually.

6) After collection, the information will be put together by the DPC. The DPC will check each information ..

a) if it is needed for legal reasons

b) if it is needed to continue to provide the service to the customer

c) if it is technically possible to correct the information. (e.g. legal archive it is not possible)

7) The DPC will instruct the responsible person of data processing (according to our record of privacy data processing) to correct all other (point 6) personal data of the requestor. If necessary the DPC will request the correction also at our service providers (e.g. Panteon)

8) The DPC will inform the requestor about the correction of his personal data, and the reasons, why some could not be corrected (Point 6).

GDPR Process for deletion requests of data subjects

GENERAL PROCESS INFORMATIONS	
Process Name	GDPR deletion requests of data subjects
Process Owner	Schaefer Alexander
Date Created	2018-05-05
Last Update by	
Last Update date	
Last revision Date	
Process Purpose	The purpose of this process is how to react on formal deletion requests of a data subjects regarding their stored personal data.

Process Flow:

1) only written requests can be accepted. Please ask for a written request.

2) every request has to be forwarded to the local Data Protection Coorinator (DPC) and to the Group CIO

3) The DPC will start the identifiaction process. The requester must be identified in such a way that we are sure that the request comes from the person for whom he or she claims to be.

A possible answer to the request could be:

We would be happy to delete the requested information! Please send us a copy of your identity card via your email address in order to identify you as a user of our services. Please black out all information except picture, name and date of birth. Only after successful verification may we forward your data to you.

4) If the person is an employee or former employee the information goes to HR department and General Manager of the country.

5) The DPC will intruct the responsible persons of personal data processing (according to our record of privacy data processing) to collect the information about the requestor.

a) If the person is a customer or user of our services (eXite, eXite Pro, TradeIT, submIT, TrustIT, BuyIT, location finder or other connected services) we have to collect the stored data manually from the services used by the requestor. In addition, if this person has accounts at our suppliers/service providers (e.g. Panteon) we have to request the information from the effected service provider.

b) we have to manually collect all information stored in local CRM system about the requestor.

c) we have to manually collect all information stored in our Billing system about the requestor.

d) if the requestor is an employee or former employee we have to manually collect all information stored in HR systems.

e) The record of privacy data processing has to be checked if any other processing can be relevant for the requestor. And if yes, also this information has to be collected manually.

6) After collection, the information will be put together by the DPC. The DPC will check each information ..

a) if it is needed for legal reasons

b) if it is needed to continue to provide the service to the customer

c) if it is technically possible to delete the information. (e.g. legal archive it is not possible)

7) The DPC will instruct the responsible person of data processing (according to our record of privacy data processing) to delete all other (point 6) personal data of the requestor. If necessary the DPC will request the deletion also at our service providers (e.g. Panteon)

8) The DPC will inform the requestor about the deletion of his personal data, and the reasons, why some could not be deleted (Point 6).

GDPR data breach process

GENERAL PROCESS INFORMATIONS	
Process Name	GDPR deletion requests of data subjects
Process Owner	Schaefer Alexander
Date Created	2018-05-06
Last Update by	
Last Update date	
Last revision Date	
Process Purpose	The purpose of this process is how to react on any possible data breach (lost data, destroyed data, hacking, unauthorized access, ...). ⚠ NOT ONLY PERSONAL DATA - THIS PROCESS IS FOR ANY DATA BREACH ⚠

Process Flow:

1) The local Data Protection Coordinator (DPC) has to informed immediatly about any possible data breach. This include:

a) Loss of data which theoretically could fall into other hands. e.g. Lost or stolen device (Laptop, PC, Handy, external Disk, USB Drive)

b) Destroyed Data (accidentally or maliciously) by internal, external persons or by programs.

c) Discovered vulnerabilities through which data could be theoretically or practically stolen.

d) Identification of possible or practical access to data by unauthorized persons.

2) If the incident happend not in Austria the local DPC has to inform the DPC of Austria without delay. ´

3) The local DPC has to collect all relevant information about the data breach.

(a) what happend

(b) when happend it

(c) which kind of data are involved (User data, customer data)

(d) how many data are effected

4) The DPC has to initiate a RISK analysis according the following table

fact	risk points
only encryped data are effected	-20
unencrypted data are effected	+20
confirmed access by unauthorized persons	+10
personal data (e.g. Name, Adress, eMail Password) of 25 or more persons	+20
personal data (e.g. Name, Adress, eMail Password) less than 25 persons	+10

critical customer transaction data (e.g. invoices) of 25 or more customers or more than 100 transactions	+20
critical customer transaction data (e.g. invoices) of less than 25 customers or less than 100 transactions.	+10
other data than personal data or customer transaction data	+5
company critical or confidential information	+10
confidential or critical data of employees	+10
critical *) personal data are involved	+41

total risk points	risk
<=20	low risk
21-29	medium risk
>=30	high risk

5) Depending on the results of the risk analysis, the following measures are to be implemented.

high risk	medium risk	low risk
Information to general manager of Austria	Information of local general manager	no further action necessary
Information to affected persons or customers	Management decision whether affected persons or customers will be informed.	
as long as not critical *) personal data are effected, no information to government agencies is necessary		
in case that critical *) personal data are involved, the local government agencies have to be informed		

*) critical personal data are: racial and ethnic origin, political opinion, religious or philosophical beliefs, health, or sexual orientation