Personal Data Incident Level

Incident Level	Data Classification	Level Description (Meeting any one of the requirements is enough for the data to be classified in that level.)	Content of Data under this Incident Level	Reference for Range of Influence or Impact Level	Punishment
A+ (High)	Top Secret	It has the same definition as "Secret" but is strictly prohibited to share it with external units, prohibited transmitting the data externally in any form or channel, including but not limited to the transmission of data via USB flash drives, e-mail, Internet, photo/photography, and paper format.	• Health information, crime record, contact information of the important related person, etc. • Including but not limited to other information with the same influence or purpose.	• Affect or stop company system or business process. • Significant revenue loss or the loss of company competitiveness. • The risk of causing major damage to the interest of the data subject.	Termination or Dismissal
A (High)	Secret	1. Personal information accessible only by personnel responsible for specific duties. 2. Personal information related to important related person in external business contact. 3. Personal information falling into the special categories. 4. Incidents informed by government agencies or ones that attract great media attention.			
B[*2] (Medium)	Confidential	1. Personal information about stakeholder; only shared within specific groups or accessible for specific purpose with authorization. 2. Personal information regarding external personnel that has already been listed.	• Contact information provided by the stakeholder [*1] or personal system information, ID number, bank account, etc. • Including but not limited to other information with the same influence or purpose.	• Company system or business process is mildly affected but does not completely stop. • Reduce the competitiveness of BU/BG or function unit or affect customer relationship. • The risk of causing severe damage to the interest of the data subject.	Major Demerit
C (Low)	Sensitive	1. Information that could be shared within business unit with authorization from the responsible manager or consent from the data subject. 2. Personal information about internal personnel; could be obtained from company internal website.	•Contact information of employees for internal use, announcement from specific internal department regarding personal information regulations. • Including but not limited to other information with the same influence or purpose.	• Company system or business process is not affected by the incident. • Does not cause noticeable business effect, but will affect individual task. • The risk of causing average damage to the interest of data subject.	Minor Demerit

Incident Level	Data Classification	Level Description (Meeting any one of the requirements is enough for the data to be classified in that level.)	Content of Data under this Incident Level	Reference for Range of Influence • or Impact Level	Punishment
D (Other)	General	1. Information that could be shared within Delta group or among all employees openly with authorization from the responsible manager or consent from the data subject.	• Resume of internal trainer, internal announcement or newsletter sent to employees of the group regarding personal information regulations. • Including but not limited to other information with the same influence or purpose.	• The risk of causing mild damage to the interest of the data subject.	Admonishment
N/A	External Public	1. Personal information that has already been disclosed to the public. 2. Personal information that can be obtained from public sources or on public occasions. 3. Personal information that has been de-identified or could not directly or indirectly indicate the data subject.	• Business card, information of contact person that is openly revealed on website, data and analysis in which the persons involved cannot be identified. • Including but not limited to other information with the same influence or purpose.	• Extremely low risk of causing damage to the interest of the data subject.	N/A

*1 Stakeholders: refer to people or groups involved in activities such as the collection, processing or utilization of personal data, including but not limited to parties, employees, manufacturers, competent authorities of Delta Group, mass media, etc.
*2 The incident classified as level A, A+ or B is deemed as a severe violation.

Personal Data Incident Notification Level

Incident Level	Data Classification	Highest Notification Level	Highest Approval Level	Processing Days (From incident discovery to preliminary incident analysis and classification conducted by Personal Data Protection Team)
A+ (High)	Top Secret	CEO/COO	BG Head/Region GM/ Corp Function Head	Within 3 working day
A (High)	Secret			
B (Medium)	Confidential	BG Head/Region GM/ Corp Function Head	BU Head/Region Plant Mgr./ Corp Function Head	Within 3 working days
C (Low)	Sensitive	BU Head/Region Plant Mgr./ Corp Function Head	Dept. Head/Plant Mgr./ Corp Function Mgr.	Within 5 working days
D (Other)	General	BU Head/Region Plant Mgr./ Corp Function Head	First Line Mgr. & Second Line Mgr.	Within 5 working days
N/A	External Public	N/A	N/A	N/A