Data Protection Office (DPO)

External Services

1. Render advisory opinion

Render advisory opinions to UP Diliman Units/Constituents

Office or Division:	Data Protection Office
Classification:	Highly Technical
Type of Transaction:	Government to Citizen
Who may avail:	All UP Diliman Students

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
1. Email/Letter/Request/Any other form of written requests or referral letter from the Chancellor	1. Requesting Party

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Submit Email/Letter/Request /Any other form of written requests or referral letter from the Chancellor	1. Acknowledge receipt Email/ Letter/Request/Any other form of written or verbal requests or referral letter from the Chancellor 1.1 Forward the request to Data Protection Officer 1.2 Draft and Finalize Advisory Opinion	None	13 Days	*1 & 1.1 Receiving Personnel* *1.2 Data Protection Officer* Data Protection Office
2. Received Advisory Opinion	2. Released Advisory Opinion	None	1 Day	*Releasing Personnel* Data Protection Office
	TOTAL:	**None**	**14 Days**	

2. Investigate security incidents and personal data breaches

Investigate security incidents and personal data breaches and if necessary, exercise breach reporting procedures in coordination with Privacy Focal Persons.

Office or Division:	Data Protection Office
Classification:	Highly Technical
Type of Transaction:	Government to Citizen
Who may avail:	All UP Diliman Students

CHECKLIST OF REQUIREMENTS	WHERE TO SECURE
1. Email the incident with all information on hand both to Data Protection Officer and the Privacy Focal Person having the jurisdiction over the unit involved	1. Requesting Party

CLIENT STEPS	AGENCY ACTION	FEES TO BE PAID	PROCESSING TIME	PERSON RESPONSIBLE
1. Email the incident with all information on hand both to Data Protection Officer and the Privacy Focal Person having the jurisdiction over the unit involved within two (2) hours	1. Acknowledged receipt of the Email 1.1 Categorization of the Incident 1.2 Investigation and identification of the Incident	None	1 Hour 1 Hour 4 Hours	*1 Receiving Personnel* Data Protection Office *1.1 Privacy Focal Person* *1.2 Unit-Level Breach Response Team*
2. Received Notification	2. If necessary, reporting to National Privacy Commission and Notification to affected Data Subjects 2.1 Containment and Eradication of the cause of Security Incident or	None	66 hours PAUSE Clock (Max 7 Days)	*2 Data Protection Officer* *2.1 to 2.4 Unit-Level Breach Response Team*

	Personal Data Breach 2.2 Restore the system or application to its working state 2.3 Update the status of the Security Incident or Personal Data Breach 2.4 Discussion of lessons learned		PAUSE Clock (Max 7 Days) 1 Day 1 Day	
TOTAL:		None	19 Days	