မူဝါဒ အကျဉ်းချုပ်

ပုဂ္ဂလိက လွတ်လပ်ခွင့်အား အကာအကွယ်ပေးသည့် အချက်အလက် ကာကွယ်ရေး ဥပဒေ။

မြန်မာနိုင်ငံနှင့် သက်ဆိုင်သည့် အကြောင်းအချက်များ

ဤမူဝါဒ အကျဉ်းချုပ်[1]တွင် **အချက်အလက်ကာကွယ်ရေးနှင့် ပုဂ္ဂလိက လွတ်လပ်ခွင့်**အား ကိုင်တွယ် ဖြေရှင်းရာတွင် အသုံးပြုနိုင်သည့် ဝေါဟာရ အသုံးအနှုန်းများ၊ ယူဆချက်များနှင့် အလေ့အကျင့်ကောင်းများ၏ ခြုံငုံချက်များကို ဖော်ပြပေးထားသည်။ ဤအခေါ်အဝေါ်များအား ကျယ်ပြန့်စွာ အသုံးပြုကြသော်လည်း အများအားဖြင့် နားလည်သဘောပေါက်မှု အားနည်းကြသည်။ ဤအကြောင်းအရာများနှင့် ပတ်သက်၍ မြန်မာနိုင်ငံတွင် ချင့်ချိန်သိရှိနားလည်သည့် (informed) ဆွေးနွေးမှုများ ပေါ်ပေါက်လာစေရန်အတွက် အားပေးရန်၊ အချက်အလက်နှင့် လူ့အခွင့်အရေးအား ကာကွယ်ပေးသည့် အချက်အလက် ကာကွယ်ရေး ဥပဒေအား ပြဋ္ဌာန်းနိုင်ရန်အတွက် မြန်မာအစိုးရ၊ ပုဂ္ဂလိကကဏ္ဍနှင့် အရပ်ဖက်လူ့အဖွဲ့အစည်းများအား ထောက်ပံ့ပေးရန် ရည်ရွယ်ခြင်း ဖြစ်ပါသည်။ ဤသို့ လုပ်ဆောင်ခြင်းအားဖြင့် စတုတ္ထအကြိမ် စက်မှုတော်လှန်ရေး (4th Industrial Revolution) အတွက် ပြင်ဆင်သည့်အနေဖြင့် E-Governance Master Plan နှင့် Digital ID အပါအဝင် မြန်မာနိုင်ငံ၏ ဒီဂျစ်တယ်ဂေဟ စနစ်အား ဖွံ့ဖြိုးစေလိုသည့် ရည်မှန်းချက်များအား ထောက်ပံ့ပေးရာရောက်သည်။ ဤစီမံကိန်းများ ထိရောက်မှု အားကောင်းစေရန်အတွက် ခိုင်မာအားကောင်းသည့် အချက်အလက်ကာကွယ်မှုဖြင့် ထောက်ပံ့ပေးထားရန် လိုအပ်သည်။

[1] Privacy International အား ကျေးဇူးတင်လိုသည်။ ဤအနှစ်ချုပ်စာတမ်းသည် Privacy International မှ ဖော်ပြထားသည့် "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection," (August 2018), နှင့် OECD, Privacy Framework (2013), the EU General Data Protection Regulation (2016/679) and the Council of Europe Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018) အစရှိသည်တို့အပေါ် အခြေခံထားသည်။ အာရှပစိဖိတ်ဒေသ၌ လျှပ်စစ်ကုန်သွယ်ရေးကို မြှင့်တင်ပေးရန် ရည်ရွယ်ပြီး လူပုဂ္ဂိုလ်များနှင့် သတင်း အချက်အလက် အသိုင်းအဝိုင်း အတွက် ပုဂ္ဂလိက လွတ်လပ်ခွင့်၏ တန်ဖိုးအား ပြန်လည်အဓိပ္ပါယ်ဖော်ပေးသည့် APEC Privacy Framework (2015) ကိုလည်း ကြည့်ပါ။ မွမ်းမံပြင်ဆင်ထားသည့် ၂၀၁၅ ခုနှစ် မူဘောင်သည် "OECD လမ်းညွှန်ချက် (၂၀၁၃)တွင် မိတ်ဆက်ထားသည့် ယူဆချက်များအပေါ် အခြေခံထားပြီး အခြားသော ဥပဒေဆိုင်ရာ အချက်အလက်များနှင့် APEC ဒေသ၏ အခင်းအကျင်းအား နားလည်၍ ထည့်သွင်းစဉ်းစားပေးထားသည်။

အချက်အလက် ကာကွယ်ပေးခြင်းဟူသည်မှာ အဘယ်နည်း။ ၎င်းသည် ပုဂ္ဂလိက လွတ်လပ်ခွင့်နှင့် မည်သို့ သက်ဆိုင်သနည်း။

အချက်အလက် အကာအကွယ်ပေးခြင်းနှင့် ပုဂ္ဂလိက လွတ်လပ်ခွင့်ဆိုင်ရာ အခွင့်အရေး[2] သည် အခြေခံအားဖြင့် ဆက်နွယ်နေသည်။[3] ပြီးပြည့်စုံသော အချက်အလက် အကာအကွယ်ပေးသည့် ချဉ်းကပ်မှုနည်းလမ်းမှာ[4] အောက်ပါ ပူးတွဲရည်မှန်းချက် (၂) ရပ်ပေါ်တွင် မူတည်လျက်ရှိသည်။

- အချက်အလက် အကာအကွယ်ပေးခြင်းအား အခြေခံ အခွင့်အရေးအဖြစ် အသိအမှတ်ပြုခြင်း သာမက ပုဂ္ဂိုလ်တိုင်းမှ မိမိ၏ ကိုယ်ပိုင် အချက်အလက်များအား ထိန်းချုပ်ခြင်းနှင့် ပြင်ဆင်သုံးစွဲခြင်း (processing) အား လုပ်ဆောင်နိုင်စေမည့် အခွင့်အရေးများအား အကာအကွယ်ပေးခြင်း။

- တာဝန်ယူမှု၊ တာဝန်ခံမှုဆိုင်ရာ စနစ်များအား တည်ထောင်ခြင်းနှင့် ကိုယ်ပိုင်အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်းနှင့် ထိန်းချုပ်ခြင်းအား လုပ်ကိုင်သည့် အဖွဲ့အစည်းများအား တာဝန်ဝတ္တရားများ ရှင်းလင်းပြတ်သားစွာ ချမှတ်ပေးခြင်း။

ဤသို့သော ပြီးပြည့်စုံသည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ချဉ်းကပ်မှု နည်းလမ်းအား ပိုမိုကျယ်ပြန့်သည့် အမျိုးသား **ဆိုက်ဘာလုံခြုံရေး နည်းဗျူဟာ**ကို ဆောင်ရွက်ရာတွင် တစ်စိတ်တစ်ပိုင်း အနေနှင့် ထည့်သွင်းလုပ်ဆောင်သင့်ပါသည်။[5]

---

[2] Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 21 of the ASEAN Human Rights Declaration တို့ကိုလည်းကြည့်ပါ။

[3] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/17/27, para. 58 (May 16, 2011).

[4] အချို့သော အခြေအနေများတွင် ပိုမိုယေဘုယျကျသည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေအား ဖြည့်ဆည်းပေးနိုင်ရန်အတွက် အခြားသော ကဏ္ဍအလိုက်ဆိုင်ရာ ပြဋ္ဌာန်းချက်များလည်း လိုအပ်လာနိုင်သည်။ (ဥပမာအားဖြင့် ဆက်သွယ်ရေး၊ ကျန်းမာရေးနှင့် ပညာရေး နယ်ပယ်များအတွက်)

[5] မြန်မာ့စီးပွားရေးကဏ္ဍ တာဝန်ယူမှုရှိရေး အထောက်အကူပြုဌာန၏ ဆိုက်ဘာလုံခြုံရေးနှင့် ဆိုက်ဘာပြစ်မှုဆိုင်ရာ မူဝါဒ အကျဉ်းချုပ်များအား ကြည့်ပါ။

အဘယ့်ကြောင့် အချက်အလက် အကာအကွယ်ပေးခြင်းအား လိုအပ်သနည်း။

တစ်ကမ္ဘာလုံးဆိုင်ရာ ဒီဂျစ်တယ် စီးပွားရေးသည် ကိုယ်ရေးကိုယ်တာ အချက်အလက်များအား အောက်ပါပုဂ္ဂိုလ်တို့ထံမှ ပိုမိုများပြားစွာ တောင်းခံခြင်း ခံနေရသည့် အခြေအနေကို ဦးတည်နေသည်။

- **အစိုးရများ** - ပုဂ္ဂိုလ်များအား သတ်မှတ်ဖော်ထုတ်ရန်နှင့် ၎င်းတို့အား ပြည်သူ့ ဝန်ဆောင်မှုများ ပေးစွမ်းရန်။
- **ကုမ္ပဏီများ -** စားသုံးသူများအတွက် ရည်ရွယ်ထားသည့် ကုန်ပစ္စည်းများနှင့် ဝန်ဆောင်မှုများကို ပေးစွမ်း ရန်။

အထက်ပါ အစိုးရများနှင့် ကုမ္ပဏီများသည် လူအများနှင့် သက်ဆိုင်သည့် အချက်အလက်များအား ပြင်ဆင်သုံးစွဲရန်၊ ၎င်းတို့နှင့် သက်ဆိုင်သည့် အခြားသော အချက်အလက်များအား ဖော်ထုတ်ရန်နှင့် အချက်အလက်များကို အသုံးပြု၍ ထိုသူများနှင့် စပ်လျဉ်းသော ဆုံးဖြတ်ချက်များအား ချမှတ်နိုင်ရန် ရည်ရွယ်၍ အချက်အလက်သုံးစွဲမှု ကျယ်ပြန့်သည့် စနစ်များ (data-intensive systems) ကို ပိုမိုများပြားစွာ အသုံးပြုလာကြသည်။

ပိုမိုကျယ်ပြန့်ဆန်းသစ်သော ကိုယ်ရေးကိုယ်တာ အချက်အလက် အသုံးပြုမှု နည်းလမ်းများသည် စီးပွားရေးနှင့် လူမှုရေးဆိုင်ရာ အကျိုးအမြတ်များကို ပိုမိုများပြားစွာ ဖြစ်ပေါ်စေသော်လည်း ပုဂ္ဂလိက လွတ်လပ်ခွင့်ဆိုင်ရာ အန္တရာယ်များကိုလည်း များပြားလာစေသည်။ စည်းမျဉ်းစည်းကမ်း သတ်မှတ်ခြင်း အပါအဝင် အချက်အလက်များအား ပေါက်ကြားခြင်း မရှိအောင် လုံခြုံစွာ ထိန်းသိမ်းထားခြင်း မရှိပါက အများပြည်သူအနေဖြင့် ဒီဂျစ်တယ်စီးပွားရေးကို ထောက်ပံ့ပေးထားသော စနစ်များအား ယုံကြည်မှု ရှိလာတော့မည် မဟုတ်ပေ။[6] အကာအကွယ်ပေးခြင်း မရှိပါက ပြစ်မှုများ ကျူးလွန်မိစေရန် အလားအလာအသစ်များ ဖြစ်ပေါ်လာနိုင်သလို ရှိရင်းစွဲ တရားမျှတမှု မရှိခြင်းနှင့် ခွဲခြားဆက်ဆံခြင်းများအား ပိုမိုဆိုးရွားလာစေနိုင်သည်။ အကျိုးဆက်အနေဖြင့် ဖွံ့ဖြိုးမှုကို တွန်းအားပေးမည့် နည်းပညာပိုင်းဆိုင်ရာ တိုးတက်မှုများ၏ ထိရောက်မှုကိုလည်း နည်းပါးစေသည်။[7]

၂၀၁၈ ခုနှစ် စက်တင်ဘာလ၌ လေ့လာထားခြင်းအရ နိုင်ငံပေါင်း ၁၀၀ ကျော်သည် ပြီးပြည့်စုံသည့် အချက်အလက် ကာကွယ်ရေးဆိုင်ရာ ဥပဒေမူဘောင်များအား ပြဋ္ဌာန်းထားပြီးဖြစ်သလို နိုင်ငံပေါင်း ၄၀ ခန့်သည် ထိုသို့သော

---

[6] ဒီဂျစ်တယ် စီးပွားရေးလောကအား လေ့လာခဲ့သည့် OECD ၏ ၂၀၁၄ ခုနှစ် စစ်တမ်းအရ အစိုးရများသည် ဖြစ်နိုင်ခြေ ၃၁ မျိုးအနက်မှ လုံခြုံရေးအား ဒုတိယအရေးကြီးဆုံး အပိုင်းအဖြစ်လည်းကောင်း ပုဂ္ဂလိက လွတ်လပ်ခွင့်အား တတိယ အရေးကြီးဆုံးအဖြစ်လည်းကောင်း သတ်မှတ်ဖော်ထုတ်ခဲ့ပြီး broadband သည် အရေးကြီးဆုံး အပိုင်း ဖြစ်နေသည်။

[7] OECD, Digital Economy Outlook (2017), p. 17

ဥပဒေများအား ပြဌာန်းနိုင်ရန် ဆောင်ရွက်လျက်ရှိသည်။[8] သို့သော် လက်ရှိအခြေအနေအရ မြန်မာနိုင်ငံ၌ ထိရောက်မှုရှိသည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများ မရှိသေးပါ။ ထို့ကြောင့် စတုတ္ထအကြိမ် စက်မှုတော်လှန်ရေးအား ကိုက်ညီနိုင်စေမည့် ၎င်း၏ ရည်မှန်းချက်အား အကောင်အထည်ဖော်နိုင်ရန် ခက်ခဲပေလိမ့်မည်။

ပုဂ္ဂလိက အချက်အလက်များသည် ဆန်းသစ်တီထွင်မှုကို အသုံးချ၍ စည်ပင်ဝပြောမှုနှင့် အခွင့်အလမ်းများအား မြှင့်တင်လျက်ရှိသည့် တစ်ကမ္ဘာလုံးအဆင့် သတင်းအချက်အလက် စီးပွားရေးလောက၏ လောင်စာ ဖြစ်သည်။ ၎င်းလောင်စာ ဆက်လက်တည်တံ့စေနိုင်ရန်မှာမူ အချက်အလက်များအား အကာအကွယ်ပေးရမည်ဟူ၍ အစိုးရများမှ နားလည်လာကြသည်။ ဥပမာအနေဖြင့် ဥရောပ သမဂ္ဂသည် ပုဂ္ဂလိက အချက်အလက်များအား ဥရောပ သမဂ္ဂမှ တတိယနိုင်ငံသို့ အခြားသော အကာအကွယ်များ မရှိဘဲ ရောက်ရှိသွားနိုင်ခြင်း ရှိ၊ မရှိနှင့် စပ်လျဉ်း၍ ဥရောပ သမဂ္ဂ ပြင်ပရှိ မည်သည့် နိုင်ငံများ၌ လုံလောက်သည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ နည်းစနစ်များ ရှိကြောင်း ဆုံးဖြတ်နိုင်ရန် ဆောင်ရွက်လျက်ရှိသည်။[9] အကယ်၍ မြန်မာနိုင်ငံ၌ သင့်တော်သည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများ မရှိလျှင်ဖြစ်စေ၊ ၎င်းဥပဒေများအား ပြီးပြည့်စုံစွာ အကောင်အထည်ဖော်ထားခြင်း မရှိလျှင်ဖြစ်စေ တစ်ကမ္ဘာလုံးအဆင့် ဒီဂျစ်တယ် စီးပွားရေးလောက၌ ဆန့်ဝင်ခြင်း မရှိနိုင်မည့် အန္တရာယ်နှင့် ရင်ဆိုင်ရပေလိမ့်မည်။[10]

အခြားတစ်ဖက်တွင်မူ အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများအား မမှန်မကန် အသုံးပြုပြီး မှားယွင်းမှုများနှင့် အဂတိလိုက်စားမှုများအား ဖုံးဖိခြင်းကို မပြုလုပ်သင့်ပေ။ သို့မဟုတ်လျှင်လည်း အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများ အနေနှင့် ကျစ်ကျစ်လျစ်လျစ်မရှိပဲ ကျယ်ပြန့်လွန်းနေပါက ကျော်ကြားသူများနှင့် ၎င်းတို့၏ လုပ်ရပ်များအား မှန်ကန်မျှတစွာ ဝေဖန်ခြင်းအား တရားစွဲဆိုခြင်း (သို့) ဟန့်တားခြင်း တို့ကို ပြုလုပ်နိုင်သည့် အနေအထားတွင်ရှိသည်။ အဆိုပါ ဥပဒေများသည် စားသုံးသူ အကာအကွယ်ပေးရေး ဥပဒေကဲ့သို့သော အချက်အလက် ကာကွယ်ခြင်းပေါ် ပိုမို၍ အခြေခံလာပြီး အရောင်းအဝယ်ကိစ္စများအား ထောက်ပံ့ပေးထားသည့် ဥပဒေများနှင့်အတူ ညှိနှိုင်း ဆောင်ရွက်သင့်ပါသည်။[11]

---

[8] အရင်းအမြစ်။ Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (Sept, 2018)

[9] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[10] UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), p. 8

[11] http://www.myanmar-law-library.org/law-library/laws-and-regulations/laws/myanmar-laws-1988-until-now/union-solidarity-and-development-party-laws-2012-2016/myanmar-laws-2014/pyidaungsu-hluttaw-law-no-10-2014-consumer-protection-law-burmese.html

မြန်မာနိုင်ငံ၌ ပြီးပြည့်စုံသည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေ ပေါ်ပေါက်လာစေရန် လိုအပ်သည့် ပြဋ္ဌာန်းချက် ၆ ရပ်

မြန်မာနိုင်ငံတွင် ပြီးပြည့်စုံသည့် အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေ[12] ပေါ်ပေါက်လာစေရန် အတွက် အခြားသော အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများတွင် ပါဝင်သော ပြဋ္ဌာန်းချက်များအား အောက်ပါအတိုင်း ထည့်သွင်းသင့်ပါသည်။

၁။ ရှင်းလင်းပြတ်သားသည့် ရည်ရွယ်ချက်နှင့် အသုံးချမည့် နယ်ပယ်အတိုင်းအတာ

ဆိုလိုသည်မှာ ဤဥပဒေသည် -

- ပုဂ္ဂလိက လွတ်လပ်ခွင့်နှင့် အခြား ဆက်စပ်အခွင့်အရေးများကို ကာကွယ်ပေးထားသော အပြည်ပြည်ဆိုင်ရာ လူ့အခွင့်အရေးများနှင့် ဖွဲ့စည်းပုံအခြေခံဥပဒေမှ ကာကွယ်ပေးမှုများကို တိုက်ရိုက် ရည်ညွှန်းထားသည့် **မှန်ကန်မျှတမှုရှိသော ရည်ရွယ်ချက်**အပေါ် အခြေခံရမည်။

- လူတစ်ဦးတစ်ယောက်အကြောင်းကို သွယ်ဝိုက်၍ သတ်မှတ်ပေးနိုင်မည့် အချက်အလက် ကဲ့သို့သော သတင်းအချက်အလက် အမျိုးအစားများစွာ အကျုံးဝင်သည့် **ပုဂ္ဂလိက အချက်အလက်အား ကျယ်ပြန့်စွာ အဓိပ္ပါယ် ဖွင့်ဆိုချက်တစ်ရပ်** ပါဝင်သင့်သည်။ ဤအဓိပ္ပါယ် ဖွင့်ဆိုချက်တွင် ကွန်ပျူတာ၊ ဖုန်း၊ IoT ကိရိယာများနှင့် စက္ကူမှတ်တမ်းများမှ တဆင့် အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်း[13] ၏ ဆင့်ကဲဖြစ်စဉ် တစ်ခုလုံး ပါဝင်သင့်သည်။

- လူမျိုး သို့မဟုတ် တိုင်းရင်းသား မျိုးရိုး၊ ဘာသာရေးဆိုင်ရာ ဆက်နွယ်မှုများ၊ ကုန်သွယ်မှု သမဂ္ဂ အဖွဲ့ဝင် အစရှိသဖြင့် ခွဲခြားဆက်ဆံမှု ခံရနိုင်ခြေရှိသည့် အကြောင်းအရာများနှင့် ပတ်သက်သည့် **ထိခိုက်လွယ်သော (sensitive) အချက်အလက်များအတွက် ပိုမိုမြင့်မားသည့် ကာကွယ်မှုများ** ပေးစွမ်းရမည်။

- ဥပဒေသည် **ပုဂ္ဂလိကနှင့် ပြည်သူပိုင် အဖွဲ့အစည်းများအတွက် သက်ဆိုင်မှု** ရှိစေရမည်။ ဥပဒေ စိုးမိုးရေး၊ အမျိုးသား လုံခြုံရေးနှင့် ထောက်လှမ်းရေး အေဂျင်စီများအတွက် ကင်းလွတ်ခွင့် မပေးစေရ။ ဥပဒေမှ

---

[12] လတ်တလော UNCTAD လေ့လာမှုအရ အစိုးရများ၊ အထူးသဖြင့် အချက်အလက် ကာကွယ်ရေး ဥပဒေများအား ပြဋ္ဌာန်းနိုင်ရန် ကြိုးပမ်းနေသည့် ဖွံ့ဖြိုးဆဲနိုင်ငံများရှိ အစိုးရများသည် အများစုအားဖြင့် ဥရောပသမဂ္ဂ၏ ယေဘုယျ အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ စည်းမျဉ်းနှင့် ကိုက်ညီသည့် ချဉ်းကပ်မှုပုံစံအား ရွေးချယ်ကြသည်။ UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), p. xii.

[13] European Commission, What is personal data?

ကင်းလွတ်ခွင့်ပေးခြင်းအား နည်းနိုင်သမျှ နည်းအောင် လုပ်ဆောင်ရမည်ဖြစ်သလို ထိုကင်းလွတ်ခွင့်ပေးထားသူများအား အများပြည်သူသိအောင် ကြေငြာပေးရမည်။[14]

• ပုဂ္ဂလိက လွတ်လပ်ခွင့်နှင့် အချက်အလက် ကာကွယ်ခြင်းအား ကာကွယ်နိုင်ရန်အတွက် အိုင်စီတီနည်းပညာများမှ တစ်ဆင့် **အစိုးရမှ စောင့်ကြပ်ကြည့်ရှုခြင်း (surveillance) အပေါ် ချမှတ်သင့်သည့် ကန့်သတ်ချက်များ၊ လိုက်နာရမည့် အချက်များ**နှင့် စပ်လျဥ်း၍ အလွန် ရှင်းလင်းပြတ်သားရမည်။[15]

• အချက်အလက် ကာကွယ်မှုများသည် တစ်ကမ္ဘာလုံးနှင့် ဆက်စပ်နေသဖြင့် အချက်အလက် ထိန်းချုပ်သူ သို့မဟုတ် ပြင်ဆင်သုံးစွဲသူ အခြေခံထားသည့် နေရာနောက်လိုက်ခြင်းထက်စာလျှင် **ပုဂ္ဂိုလ် တစ်ဦးတစ်ယောက်၏ အချက်အလက်များကိုသာ** အခြေခံသင့်ပါသည်။

၂။ အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ အခြေခံမှုများအား ကိုင်တွယ်ဖြေရှင်းရန် တိကျသေချာသည့် ဥပဒေဆိုင်ရာ လိုအပ်ချက်များအား သတ်မှတ်ခြင်း

အရေးပါ၍ အသိအမှတ်ပြုခြင်း ခံရသည့် အခြေခံမှုများ[16] တွင် အောက်ပါတို့ ပါဝင်သည်။

• **တရားမျှတ၍ ဥပဒေနှင့် ညီညွတ်ကာ ပွင့်လင်းမြင်သာခြင်း** ။ ဥပဒေနှင့်အညီ မျှတသည့် နည်းလမ်းများဖြင့် စုဆောင်းထားသည့် ပုဂ္ဂလိက အချက်အလက်များအား ကောက်ယူမှုအပေါ် ကန့်သတ်ချက်များ ရှိသင့်သည်။ အချက်အလက် စုဆောင်းခြင်းအား ပွင့်လင်းမြင်သာစွာ လုပ်ဆောင်ရမည်၊ လူပုဂ္ဂိုလ်များအား ၎င်းတို့၏ အချက်အလက်များအား မည်သူက မည်သို့ ပြင်ဆင်သုံးစွဲမည်ဖြစ်ကြောင်း ရှင်းလင်းစွာ အသိပေးရမည်။ လျှို့ဝှက်ထားသည့် အချက်အလက် ပြင်ဆင်သုံးစွဲခြင်းများ မရှိသင့်ပါ။

---

[14] OECD, Privacy Framework (2013).

[15] Myanmar Centre for Responsible Business, "Sector Wide Impact Assessment of Myanmar's ICT Sector, Recommendations, Annex I: Lawful Interception and Government Access to User Data: The Characteristics of a Rights-Respecting Model" (2016), p. 35 and UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), pp. 15-16 နှင့် "emerging 'test' for achieving a balance between data protection and surveillance.", p. 59 အားကြည့်ပါ။

[16] အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများ စီစဥ်ရေးဆွဲရာတွင် နိုင်ငံများမှ အတုယူသင့်သည့်ဟု အသိအမှတ်ပြုခြင်း ခံထားရသော အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ အခြေခံမှုများ အစုံလိုက်ရှိကြောင်း အသိအမှတ်ပြုထားသည့် UNCTAD ၏ Data protection regulations and international data flows: Implications for trade and development, (2016) - pp. 56-57 အား ကြည့်ပါ။

- **ရည်ရွယ်ချက် အကန့်အသတ်**။ ပုဂ္ဂလိက အချက်အလက်များအား တိကျသေချာ၍ တရားဝင်သည့် ရည်ရွယ်ချက်အတွက်သာ အသုံးချရမည်။ အဆိုပါ ရည်ရွယ်ချက်အား အချက်အလက် စုဆောင်းသည့် အချိန်၌ ရှင်းလင်းစွာ ထုတ်ဖော်ပြောရမည်။ သဘောတူညီထားသည့် ရည်ရွယ်ချက်များအတွက်သာ စုဆောင်းထားသည့် အချက်အလက်များအား အသုံးပြုရမည်။ ရည်ရွယ်ချက်တစ်ခုအတွက် အချက်အလက် စုဆောင်း၍ အသိပေးခြင်း၊ သဘောတူညီချက် ရယူခြင်း (သို့) အကြောင်းအကျိုး ရှင်းပြခြင်း မရှိဘဲ အခြားသော ရည်ရွယ်ချက်အတွက် အချက်အလက်များအား အသုံးပြုခြင်း မပြုရ။

- **အချက်အလက် နည်းပါးခြင်း**။ ဖြစ်နိုင်သမျှ အချက်အလက် စုဆောင်းရာ၌ အနည်းဆုံး ပမာဏကိုသာ စုဆောင်းရမည်။

- **တိကျသေချာခြင်း**။ ပုဂ္ဂလိက အချက်အလက်များသည် မှန်ကန်တိကျ၍ ပြည့်စုံရမည်ဖြစ်သလို မမှန်ကန်ခြင်း မရှိစေရန် အချိန်နှင့်အမျှ ပြောင်းလဲမွမ်းမံရမည်။

- **သိုလှောင်မှု ကန့်သတ်ချက်**။ အချက်အလက် ကောက်ခံစဉ် ရည်ရွယ်သည့် အချိန်ကာလ အပိုင်းအခြားအထိသာ သိုလှောင်သိမ်းဆည်းသင့်ပြီး ၎င်းထက် ပိုမို ကြာမြင့်စွာ သိမ်းဆည်းခြင်းမျိုး မပြုသင့်ပါ။

- **ကျင့်ဝတ်နှင့် လျှို့ဝှက်ထားခြင်း**။ ပုဂ္ဂလိက အချက်အလက်များအား ကြောင်းကျိုးခိုင်လုံသည့် လုံခြုံရေး အကာအကွယ်များဖြင့် ဆုံးရှုံးခြင်း၊ တရားမဝင် ရယူသုံးစွဲခြင်း၊ ဖျက်ဆီးခြင်း၊ အသုံးပြုခြင်း၊ မွမ်းမံပြင်ဆင်ခြင်း (သို့) ထုတ်ဖော်ကြေငြာခြင်း အစရှိသည်တို့ မဖြစ်စေရန် ထိန်းသိမ်းကာကွယ်ပေးရမည်။

- **တာဝန်ယူမှု၊ တာဝန်ခံမှု**။ ပုဂ္ဂလိက အချက်အလက်များအား ပြင်ဆင်သုံးစွဲသည့် မည်သည့် အဖွဲ့အစည်း မဆို၊ အချက်အလက် ထိန်းချုပ်သူအနေဖြင့် ဖြစ်စေ (သို့) အချက်အလက် ပြုပြင်ပြောင်းလဲသူအနေဖြင့် ဖြစ်စေ၊ ဥပဒေနှင့် အညီ လိုက်နာဆောင်ရွက်ရန် တာဝန်ရှိသည်။ ၎င်းတို့သည် အများပြည်သူ၏ ပုဂ္ဂိုလ်ရေး လွတ်လပ်ခွင့်အား လေးစားကြောင်း စည်းကမ်းကြပ်မတ်သူများနှင့် ပုဂ္ဂိုလ်များထံ ရှင်းပြနိုင်ရမည်၊ ပြသနိုင်ရမည်၊ အထောက်အထားပြနိုင်ရမည်။

၃။ အချက်အလက် ကောက်ခံခြင်းခံရသည့် ပုဂ္ဂိုလ်များ၏ အခွင့်အရေးများအား ကာကွယ်ရန် တိကျသည့် ဥပဒေအရ လိုအပ်ချက်များ ချမှတ်ခြင်း

အောက်ပါတို့သည် အချက်အလက်များ ကောက်ခံခြင်း ခံရသည့် ပုဂ္ဂိုလ်များ[17] ၏ အရေးပါ၍ ကောင်းမွန်စွာ အသိအမှတ်ပြုထားပေးသည့် အခွင့်အရေးများ ဖြစ်သည်။ ပုဂ္ဂိုလ်များတွင် အောက်ပါအခွင့်အရေးများ ရှိသည်။

- **သတင်းအချက်အလက် ရပိုင်ခွင့်** ။ ၎င်းတို့၏ အချက်အလက်များအား မည်သူတို့က မည်သည့် ရည်ရွယ်ချက်ဖြင့် အသုံးပြုနေကြောင်း အသိပေးခြင်း ခံရမည်။

- **ရယူသုံးစွဲမှုဆိုင်ရာ ရပိုင်ခွင့်**။ အချက်အလက် ထိန်းချုပ်သူသည် ၎င်းတို့နှင့် ပတ်သက်၍ အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်း ရှိမရှိ၊ ပြင်ဆင်သုံးစွဲခြင်း၏ ရည်ရွယ်ချက်၊ ပြင်ဆင်သုံးစွဲရခြင်း၏ တရားဝင် အကြောင်းရင်း၊ အချက်အလက် ရရှိခဲ့သည့် နေရာ၊ အချက်အလက်များအား မည်သူတို့နှင့် မျှဝေထားပြီးဖြစ်ကြောင်း၊ အချိန်မည်မျှကြာအောင် သိုလှောင် သိမ်းဆည်းထားမည်ဖြစ်ကြောင်း၊ သတင်းအချက်အလက်များ၏ မိတ္တူအား သိမ်းဆည်းထား၍ အချက်အလက်များအား အသုံးပြုကာ profiling ပြုလုပ်ခြင်းနှင့် အလိုအလျောက် ဆုံးဖြတ်ချက် ချမှတ်ခြင်းအား ဆောင်ရွက်ခြင်း ရှိမရှိ အစရှိသည်တို့နှင့် စပ်လျဉ်းသည့် သတင်းအချက်အလက်များအား ရယူခြင်း။

- **ပြင်ဆင်ခွင့်၊ ပိတ်ပင်ခွင့်၊ ဖျက်ပိုင်ခွင့်**။ အချက်အလက်များသည် အချိန်နှင့် အညီ မှန်ကန်တိကျ၍ ပြီးပြည့်စုံစေရန်နှင့် သို့မဟုတ်ပါက လုံးဝ ပိတ်ပင်ခြင်း သို့မဟုတ် ဖျက်ဆီးပစ်ခြင်း တို့ကို လုပ်ဆောင်ခြင်း။

- **ဆန့်ကျင်ပိုင်ခွင့်**။ ၎င်းတို့၏ အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်းအား မည်သည့် အချိန်တွင်မဆို ဆန့်ကျင်ပိုင်ခွင့် ရှိသည်။ အချို့သော ဆန့်ကျင်ပိုင်ခွင့်များသည် ဥပမာအနေဖြင့် တိုက်ရိုက် မားကက်တင်း ပြုလုပ်ခြင်းကဲ့သို့သော အခြေအနေများတွင် အကြွင်းမဲ့ဖြစ်သည်။ အခြားသော အချက်အလက် ပြင်ဆင်သုံးစွဲခြင်းလုပ်ငန်းများအား လိုအပ်သလို အကြောင်းရင်း ရှင်းပြနိုင်ရမည်။

---

[17] OECD Recommendation: [Digital Security Risk Management for Economic and Social Prosperity]() (2015) အားကြည့်ပါ။

• **အချက်အလက် သယ်ဆောင်ပိုင်ခွင့်**။ ၎င်းတို့၏ ပုဂ္ဂလိက အချက်အလက်များအား အခြား ဝန်ဆောင်မှုထံသို့ အဆိုပါ ပုဂ္ဂိုလ်၏ ခွင့်ပြုချက် ရယူ၍ ဖြန့်ဖြူးပေးခြင်း။

• **လူများ၏ အမူအကျင့်များကို မှတ်တမ်းတင်ခြင်း၊ လေ့လာဆန်းစစ်ခြင်း (Profiling) နှင့် အလိုအလျောက် ဆုံးဖြတ်ချက် ချမှတ်ခြင်းဆိုင်ရာ ရပိုင်ခွင့် (Automated Decision Making)** ။ အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်း၊ လူများ၏ အမူအကျင့်များကို မှတ်တမ်းတင်ခြင်း၊ လေ့လာဆန်းစစ်ခြင်း profiling ပြုလုပ်ခြင်းနှင့် လူသားများမှ ပါဝင်ဆောင်ရွက်ခြင်း မရှိဘဲ အလိုအလျောက် ဆုံးဖြတ်ချက် ချမှတ်ခြင်း မရှိစေရန် (အကယ်၍ ထိုသို့ ဆုံးဖြတ်ချက် ချမှတ်ခြင်းသည် သိသာစွာ သက်ရောက်မှုရှိပါက) ဆန့်ကျင်ပိုင်ခွင့်။

• **ထိရောက်မှု ရှိသည့် နစ်နာကြေး၊ လျော်ကြေးပေးခြင်းနှင့် တာဝန်** ။ အချက်အလက် ထိန်းချုပ်သူ နှင့်/သို့ အချက်အလက် ပြင်ဆင်သုံးစွဲခြင်းအတွက် ထိရောက်မှုရှိသည့် နစ်နာကြေးပေးခြင်း၊ ဆုံးရှုံးမှု ခံစားရသည့်အတွက် လျော်ကြေးပေးခံရခြင်း။

၄။ ပုဂ္ဂလိက အချက်အလက်များအား ပြင်ဆင်သုံးစွဲခြင်းအတွက် အကြောင်းပြချက်များအား ပြတ်သားစွာ အကန့်အသတ်ဖြင့်သာ ပေးခြင်း

ပုဂ္ဂလိက အချက်အလက်များအား ပြင်ဆင်သုံးစွဲရသည့် အကြောင်းရင်းများအား ကန့်သတ်ထားသင့်ပြီး ဥပဒေ၌ ထည့်သွင်းပြဋ္ဌာန်းထားရမည်ဖြစ်သည်။

• **သဘောတူခွင့်ပြုချက်** ။ သဘောတူခွင့်ပြုချက်ဟူသည် ပုဂ္ဂိုလ်တစ်ဦးအတွက် တိကျပြတ်သား၍ ကိုယ်ပိုင်ဆုံးဖြတ်ရသည့် လုပ်ငန်းစဉ် ဖြစ်သင့်ပြီး လွတ်လပ်စွာ ပေးအပ်၍ တိကျသေချာပြီး ချင့်ချိန်တွေးခေါ်ကာ ပြတ်သားမှု ရှိရမည်။ ဥပမာအားဖြင့် "သဘောတူ ခွင့်ပြုချက်" ဟူသည် အလိုလို ရွေးချယ်ထားပြီးသား အကန့်၌ အမှန်ခြစ် ခြစ်ထားခြင်းအား ပယ်ဖျက်ရသည်မျိုး မဖြစ်သင့်ဘဲ ကိုယ်ပိုင် ဆုံးဖြတ်ချက်မျိုး ဖြစ်သင့်သည်။ "သဘောတူ ခွင့်ပြုချက်" ဟူသည် ပြန်လည် ရုပ်သိမ်းရန်လည်း လွယ်ကူစေရမည်။

• ပုဂ္ဂလိက အချက်အလက်သည် အောက်ပါအကြောင်းအရာများအတွက် လိုအပ်သည်။

  o ပုဂ္ဂိုလ်တစ်ဦးနှင့် စာချုပ် ချုပ်ဆိုရန်အတွက်လည်းကောင်း (သို့) စာချုပ်ချုပ်ဆိုရန် ခြေလှမ်းများ ချမှတ်ရန်အတွက်လည်းကောင်း။

  o ဥပဒေဆိုင်ရာ တာဝန်များအား လိုက်နာဆောင်ရွက်ခြင်း

၀ အများပြည်သူ၏ အကျိုးအတွက် လုပ်ငန်းတစ်ရပ်အား ဆောင်ရွက်ခြင်း (သို့) ထိန်းချုပ်သူ၌ တရားဝင်ရှိသည့် တာဝန်၊ ဥပမာအားဖြင့် ပြည်သူ့ကျန်းမာရေး အကြောင်းရင်းများအတွက်။

၀ အချက်အလက် ထိန်းချုပ်သူမှ လုပ်ဆောင်သည့် ကျိုးကြောင်းညီညွတ်သည့် စိတ်ဝင်စားမှု။

၀ အချက်အလက် ကောက်ခံခြင်း ခံရသည့်သူများ၏ အဓိက အကျိုးအမြတ်အတွက်။

၅။ အချက်အလက် ထိန်းချုပ်သူများနှင့် ပြင်ဆင်ပြောင်းလဲသူများအတွက် တိကျသေချာသည့် ဥပဒေဆိုင်ရာ လိုအပ်ချက်များအား ချမှတ်ခြင်း

ဥပဒေအရ လိုက်နာကျင့်သုံးရန် တာဝန်ရှိသူများနှင့် ပုဂ္ဂလိက အခွင့်အရေးများအား ကာကွယ်ပေးရန် နှင့် ဥပဒေနှင့် ညီညွတ်စေရန်အတွက် သက်ဆိုင်သည့် တာဝန်များနှင့် ကတိကဝတ်များအား ရှင်းလင်းပြတ်သားစွာ သတ်မှတ်ဖော်ထုတ်ရမည်။ ၎င်းတို့ထဲတွင် အချက်အလက်များအား လုံခြုံစွာ ထိန်းသိမ်းစောင့်ရှောက်ရမည့် တာဝန်လည်း ပါဝင်သင့်သည်။ အကယ်၍ ဥပဒေအား ချိုးဖောက်ခြင်းများ ရှိခဲ့သော် ၎င်းတို့အား စုံစမ်းစစ်ဆေး၍ အာဏာရှင်များနှင့် အချက်အလက်များ ခိုးခံရသည့် ပိုင်ရှင်ထံသို့ပါ တင်ပြရမည်ဖြစ်သည်။

၆။ အချက်အလက် ကာကွယ်ခြင်းအတွက် လွတ်လပ်၍ အမှီအခိုကင်းသည့် ကြီးကြပ်ရေးမှူး ခန့်အပ်ခြင်း

အချက်အလက် ကာကွယ်ခြင်းဆိုင်ရာ ဥပဒေများရှိသည့် နိုင်ငံများ၏ ၉၀% သည် အချက်အလက် ကာကွယ်ခြင်းအတွက် လွတ်လပ်၍ အမှီအခိုကင်းသည့် ကြီးကြပ်ရေးမှူးများအား ခန့်အပ်ထားကြသည်။[18] ၎င်းတို့သည် စုံစမ်းစစ်ဆေးရန်၊ တိုင်ကြားချက်များအား လက်ခံ၍ တုံ့ပြန်ရန်နှင့် အကြံဉာဏ်များ၊ သတင်းအချက်အလက်များပေးရန်အပြင် အများပြည်သူ သိရှိနားလည်မှုကို မြှင့်တင်ပေးရန် တာဝန်ရှိသည်။ ပိတ်ဆို့မှုများ ချမှတ်ရန်၊ အုပ်ချုပ်ရေးပိုင်းဆိုင်ရာ ဒဏ်ကြေးများ၊ ပြစ်မှုဆိုင်ရာ ပိတ်ဆို့မှုများနှင့် ကုမ္ပဏီများ၏ ဒါရိုက်တာများအပေါ် တိုက်ရိုက်တာဝန်များ ချမှတ်ရန် အာဏာရှိသည်။

[18] Privacy International, "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection," (August 2018), p. 85. See also UNCTAD study, p. xii.